

Contents

[Microsoft 365 for enterprise documentation and resources](#)

[Microsoft 365 for enterprise overview](#)

[Networking](#)

[Roadmap](#)

[Plan](#)

[Microsoft 365 networking connectivity overview](#)

[Microsoft 365 network connectivity principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning with ExpressRoute for Office 365](#)

[Plan for network devices that connect to Microsoft 365 services](#)

[Network and migration planning for Microsoft 365](#)

[Deploy](#)

[Add a domain](#)

[Configure endpoints to bypass](#)

[Office 365 IP Address and URL Web service](#)

[Additional endpoints not included in the Web service](#)

[Additional network security requirements for Office 365 GCC High and DOD](#)

[DNS records for Office 365 DoD](#)

[DNS records for Office 365 GCC High](#)

[Content Delivery Network \(CDN\) Quickstart](#)

[Use the CDN with SharePoint Online](#)

[Optimize connectivity for remote users](#)

[Overview of VPN split tunneling](#)

[Common VPN split tunneling scenarios](#)

[Implementing VPN split tunneling](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Stream and live events in VPN environments](#)

[Microsoft 365 optimization for China users](#)

[Optimizing Microsoft 365 traffic for remote workers with the native Windows 10](#)

VPN client

ExpressRoute for Office 365

Implementing ExpressRoute

Routing with ExpressRoute for Office 365

Manage

Office 365 endpoints

Microsoft 365 endpoints

Managing Office 365 endpoints

Worldwide endpoints

U.S. Government DoD endpoints

U.S. Government GCC High endpoints

Office 365 operated by 21Vianet endpoints

Content delivery networks

IPv6 support in Office 365 services

NAT support with Office 365

Network requests in Office for Mac

Network planning and performance tuning

Monitor connectivity

Managing ExpressRoute

Microsoft 365 Networking Partner Program

Tenant

Roadmap

Plan

Subscriptions, licenses, accounts, and tenants

Plan for third-party SSL certificates

Setup guides

Integration

Integrated Apps and Azure AD

Integration with on-premises

Azure integration

Azure ExpressRoute

Hybrid modern authentication

Prerequisites for Skype for Business Server and Exchange Server

Configure Exchange Server

Configure Skype for Business

Remove or disable for Skype for Business and Exchange

Office 2013, Office 2016, and Office 2019 client apps

Tenant isolation in Microsoft 365

Isolation and Access Control in Azure Active Directory

Monitoring and Testing Tenant Boundaries

Resource Limits

Isolation and Access Control

Deploy

Add a domain

Manage

Microsoft 365 service health status

Microsoft 365 monitoring

Exchange Online monitoring

Service advisories for Mailbox utilization

Service advisories for eDiscovery throttling

Service advisories for MRS source delays

Microsoft 365 Apps monitoring

Microsoft 365 Teams monitoring

Setup guides

Multiple tenants

Inter-tenant collaboration

Cross-tenant mailbox migration

Cross-tenant identity mapping

Cross-tenant OneDrive migration

Tenant-to-tenant migrations

Multi-geo

Microsoft 365 Multi-Geo

Teams multi-geo

OneDrive and SharePoint multi-geo

Exchange Multi-Geo

Plan

- Plan for multi-geo

- Administration experience

- User experience

Deploy

- Configure multi-geo

- Configure preferred data location

- Configure search

Manage

- Administering a multi-geo environment

- Manage SharePoint quotas

- Move a OneDrive site

- Move a SharePoint site

- Add or remove a geo administrator

- Restrict content to a geo location

- Configure Microsoft 365 Multi-Geo eDiscovery

- Create a group with a specific PDL

- Delete a geo location

- Enabling SharePoint Multi-Geo in your satellite geo location

- Administering Exchange Multi-Geo

Move to a new Microsoft 365 datacenter geo

- How to request your data move

- During and after your data move

- Data move general FAQ

- Where customer data is stored

- Data locations for the European Union

Identity

Overview

- Step 1. Determine your identity model

- Step 2. Protect your privileged accounts

- Step 3. Protect your user accounts

Step 4. Deploy your identity model

- Cloud-only identity

- Hybrid identity

 - Prepare for directory synchronization

 - Prepare a non-routable domain for directory synchronization

 - Set up directory synchronization

- Hybrid solutions

 - Overview

 - Use Azure Active Directory for SharePoint Server 2016 authentication

 - Connect an on-premises network to an Azure virtual network

 - Deploy a directory synchronization server in Azure IaaS

 - Deploy high availability federated authentication in Azure

 - Phase 1 - Configure Azure

 - Phase 2 - Configure domain controllers

 - Phase 3 - Configure AD FS servers

 - Phase 4 - Configure web application proxies

 - Phase 5 - Configure federated authentication

 - SharePoint Server 2013 Disaster Recovery in Microsoft Azure

Manage

- User accounts

 - User accounts

 - Add several users at the same time

- Licenses

- Passwords

- Groups

- Governance

- Directory synchronization

 - View status

 - Identify errors

 - Fix problems

 - Turn it off

Client and server software

- Roadmap

Architectural models for SharePoint, Exchange, Skype for Business, and Lync

Plan your upgrade

Office 2013

Upgrade from Office 2013 clients and servers

Office 2013 desktop

Exchange Server 2013

SharePoint 2013

Lync Server 2013

Project Server 2013

Office 2010

Upgrade from Office 2010 servers and clients

Office 2010 desktop

Exchange 2010

SharePoint 2010

Lync Server 2010

Project Server 2010

Office 2007

Upgrade from Office 2007 servers and clients

Office 2007 desktop

Exchange 2007

SharePoint 2007

Office Communications Server

PerformancePoint Server 2007

Project Server 2007

Compliance

Security

Cloud services

Roadmap

Deploy

Get ready

External collaboration

Exchange Online

SharePoint

Microsoft Teams

Meetings and conferencing

Teams voice

Yammer

Activate rights management

Configuring release options

Train your users

Manage

How to check service health

Support options

Exchange Online

SharePoint

Microsoft Teams

Yammer

Performance and tuning

Tune Microsoft 365 performance

Performance tuning using baselines and performance history

Tune Exchange Online performance

Tune SharePoint performance

Introduction to performance tuning for SharePoint

Diagnosing performance issues with SharePoint

Tune Project Online performance

Performance troubleshooting plan

Windows 10

How to check release health

Deploy and update

Microsoft 365 Apps for enterprise

Surface devices

Device management

Roadmap

Microsoft Edge

Deployment and update channel example configurations

Overview

Broad deployment of the latest releases

Manage Microsoft 365 with PowerShell

Get started

Why you need to use PowerShell

Connect to Microsoft 365 with PowerShell

Connect to all Microsoft 365 services in a single Windows PowerShell window

Create reports with PowerShell

Cmdlet references for Microsoft 365 services

PowerShell community resources

User accounts, passwords, licenses, and groups

User accounts

Create

View

Configure properties

Assign admin roles

Delete and restore

Block

Passwords

Licenses and services

View licenses and services

View licensed and unlicensed users

Assign licenses to user accounts

View account license and service details

Remove licenses from user accounts

Disable access to services

Disable access to Sway

Disable access to services while assigning user licenses

Groups

Manage security groups

Maintain security group membership

- Manage Microsoft 365 groups

- Manage Folders and Rules feature in Microsoft 365 Groups

Manage SharePoint

- Create SharePoint Online sites and add users

- Manage SharePoint Online users and groups

- Manage SharePoint Online site groups

Manage Exchange Online

- Use PowerShell to migrate email to Microsoft 365

- Use PowerShell to perform a cutover migration to Microsoft 365

- Use PowerShell to perform an IMAP migration to Microsoft 365

- Use PowerShell to perform a staged migration to Microsoft 365

- Manage Microsoft 365 with Windows PowerShell for Delegated Access partners

- Manage Microsoft 365 tenants with Windows PowerShell for Delegated Access partners

- Add a domain to a client tenancy with Windows PowerShell for Delegated Access partners

- Connect to Exchange Online via remote Windows PowerShell for Delegated Access partners

- Retrieve customer reporting data via Windows PowerShell for Delegated Access partners

Manage Microsoft Teams

- Manage add-ins with Centralized Deployment PowerShell

Windows and Office 365 deployment lab kit

Test Lab Guides

- Base configuration

- Lightweight

- Simulated enterprise

Identity

- Password hash synchronization

- Pass-through authentication

- Federated authentication

- Azure AD Seamless Single Sign-on

- Multifactor authentication

Protect global administrator accounts

Password writeback

Password reset

Automatic licensing and group membership

Azure AD Identity Protection

Identity and device access

- Cloud-only

- Password hash sync

- Pass-through authentication

Mobile device management

- Enroll iOS and Android devices

- Device compliance policies

Information protection

- Increased Microsoft 365 security

- Data classification

- Privileged access management

Contoso case study

- Overview

- Contoso IT infrastructure and needs

- Networking

- Identity

- Windows 10 Enterprise

- Microsoft 365 Apps for enterprise

- Mobile device management

- Information protection

- Security summary

Microsoft 365 architecture and solutions

Enterprise Business Continuity Management (EBCM) with cloud services

- Customer and cloud partner EBCM responsibilities

- Microsoft 365 cloud services resiliency

- Developing your continuity plan

- Service incident mitigation scenarios

[Navigation guide](#)

[Microsoft 365 for Business](#)

Microsoft 365 for enterprise overview

10/28/2022 • 4 minutes to read • [Edit Online](#)

Microsoft 365 for enterprise is a complete, intelligent solution that empowers everyone to be creative and work together securely.

Microsoft 365 for enterprise is designed for large organizations, but it can also be used for medium-sized and small businesses that need the most advanced security and productivity capabilities.

Components

Microsoft 365 for enterprise consists of:

SERVICES	DESCRIPTION
Local apps and cloud-based apps and productivity services	Includes both Microsoft 365 Apps for enterprise, the latest Office apps for your PC and Mac (such as Word, Excel, PowerPoint, Outlook, and others), and a full suite of online services for email, file storage and collaboration, meetings, and more.
Windows 10 Enterprise	Meets the needs of both large and midsize organizations. It's the most productive and secure version of Windows for users. For IT professionals, it also provides comprehensive deployment, device, and app management.
Device management and advanced security services	Includes Microsoft Intune, which is a cloud-based enterprise mobility management service that helps enable your workforce to be productive while protecting your organization data.

Plans

Microsoft 365 for enterprise is available in three plans.

PLAN NAME	CAPABILITIES
E3	Access the Microsoft 365 core products and features to securely enhance workplace productivity and drive innovation.
E5	Access the Microsoft 365 latest products and features. These include Defender for Office 365, security tools, and collaboration tools. This plan includes all E3 capabilities, plus advanced security, voice, and data analysis tools.
F3	Connect with your first-line workers through purpose-built tools and resources that they can use to help them do their best work.

If you have Microsoft 365 E3, you can also get these add-ons:

- Identity & Threat Protection

- Information Protection & Compliance
- [Microsoft 365 E5 Compliance](#)
- Microsoft 365 E5 Insider Risk

Microsoft 365 E3 users can use these add-ons to take advantage of some of the additional features Microsoft 365 E5 includes.

For more information, see [Features and capabilities for each plan](#).

Get the big picture

The [Microsoft 365 for enterprise poster](#) is a central location for you to view:

- The benefits of Microsoft 365 for enterprise, and how apps and services map to its value pillars.
- Microsoft 365 for enterprise plans and which components they contain.
- The key components of the Microsoft modern workplace, which Microsoft 365 for enterprise enables.
- The [Microsoft 365 Productivity Library](#) and representative scenarios for some common organization departments.

Microsoft 365 for enterprise

A complete, intelligent solution that empowers everyone to be creative and work together securely.

Benefits

Unlocks creativity

Built for teamwork

Integrated for simplicity

Intelligent security

Local and cloud productivity services

Microsoft 365 Apps for enterprise

Exchange Online, SharePoint Online, Skype for Business, Microsoft Teams, Yammer, Microsoft 365 Apps for enterprise

Microsoft 365 Apps for enterprise deployment and updates

Office 365 Advanced Threat Protection, Office 365 Multi-Factor Authentication, SharePoint Online and Exchange Online content search, Microsoft 365 Defender, Microsoft 365 Information Protection (IP), Data Loss Prevention (DLP)

Windows 10 Enterprise

Windows 10 deployment with upgrade in place and hybrid and updates

Windows Defender Advanced Threat Protection (ATP), Windows Hello for Business, Windows Information Protection (WIP)

Device management and advanced security services

Auto enrollment of Windows PCs and devices

Microsoft Intune, device-based conditional access policies, Azure AD Password Security, Microsoft Defender for Cloud, Microsoft Defender for Office 365, Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for IoT, Microsoft Defender for Storage, Microsoft Defender for Teams, Microsoft Defender for XDR, Microsoft Defender for Zero Trust, Microsoft

You can also [download a copy of the poster](#).

Transition your entire organization

To get a better picture about how to move your entire organization to the products and services in Microsoft 365 for enterprise, see the [transition poster](#).

Microsoft			
Transition Your Organization to Microsoft 365 for enterprise			
Check the boxes for what you have and follow the rows to digitally transform your business.			
From	To	Benefits	Guidance
Windows ☐ Windows 7* ☐ Windows 8.1	Windows 10	Most modern, secure Windows ever	 aka.ms/m365w10
Office client ☐ Office 2010*** ☐ Office 2013 ☐ Office 2016	Microsoft 365 Apps for enterprise	Ongoing updates include the latest features	 aka.ms/m365o10
Office servers ☐ Exchange Server 2010*** ☐ Exchange Server 2013 ☐ Exchange Server 2016	Exchange Online	Scalable, available, secure, and always up to date, with built-in compliance and information protection	 aka.ms/m365e10
☐ SharePoint Server 2010*** ☐ SharePoint Server 2013 ☐ SharePoint Server 2016	SharePoint Online	Teamwork and collaboration across your organization	 aka.ms/m365s10
☐ Lync Server 2010*** ☐ Lync Server 2013 ☐ Skype for Business Server 2015	Microsoft Teams	Real-time meetings and collaboration across your organization	 aka.ms/m365l10
* Reached end of support on January 14, 2020 ** Reached end of support on October 13, 2020 *** Reached end of support on April 13, 2021 **** With Microsoft 365 E5 or E3 with the Identity & Threat Protection offering ***** With Microsoft 365 E5 or E3 with the Information Protection & Compliance offering			
For more information, visit aka.ms/m365deploy .		© 2019 Microsoft Corporation. All rights reserved.	

This two-page poster is a quick way to inventory your existing infrastructure. It helps you to find guidance and move to the corresponding product or service in Microsoft 365 for enterprise. It includes Windows and Office products and other infrastructure and security elements, such as device management, identity, and information and threat protection.

End of support for Windows 7 and Office 2010 clients and servers

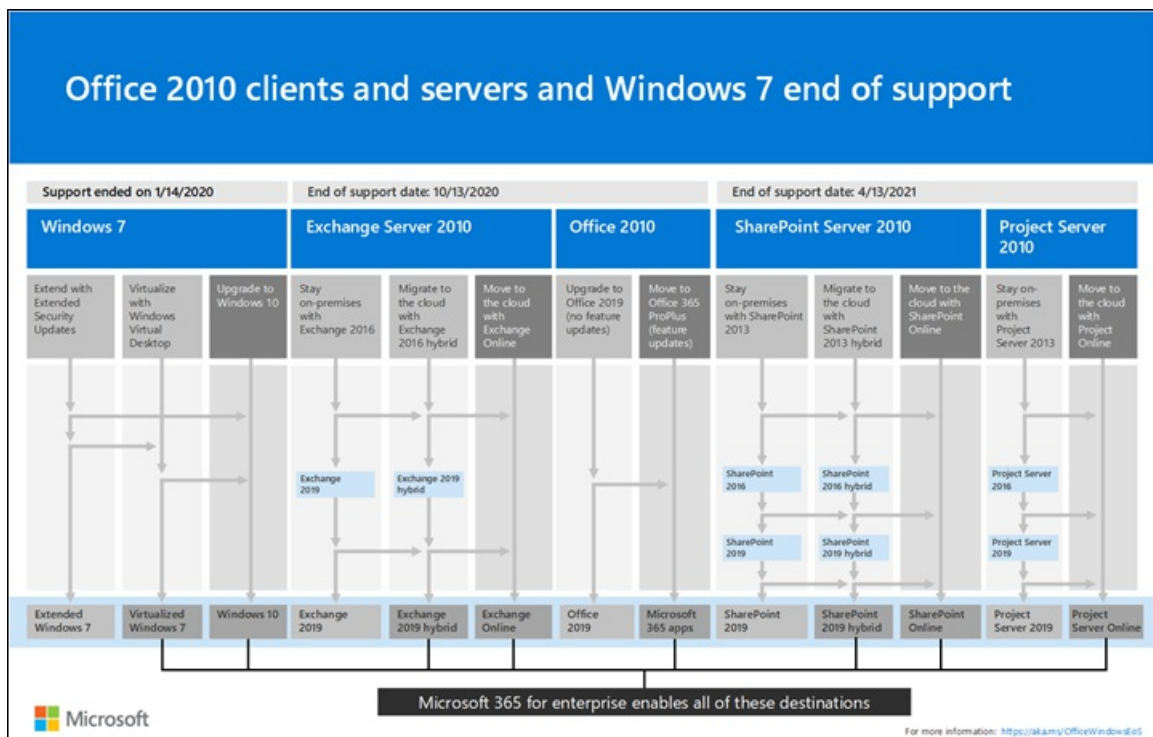
Windows 7 reached end of support on **January 14, 2020**.

These products reached end of support on **October 13, 2020**:

- [Office 2010](#)
- [Exchange Server 2010](#)

[SharePoint Server 2010](#) will reach end of support on **April 13, 2021**.

For a visual summary of the upgrade, migrate, and move-to-the-cloud options for these products, see the [end of support poster](#).



This one-page poster is a quick way to understand the various paths you can take to prevent Windows 7 and Office 2010 client and server products from reaching end of support, with preferred paths and support in Microsoft 365 for enterprise highlighted.

You can also [download this poster](#) and print it in letter, legal, or tabloid (11 x 17) formats.

Plan for and deploy

There are three ways to plan for and deploy the products, features, and components of Microsoft 365 for enterprise:

- In partnership with FastTrack

With FastTrack, Microsoft engineers help you move to the cloud at your own pace. See [FastTrack for Microsoft 365](#).

- With the help of Microsoft Consulting Services or a [Microsoft partner](#)

Consultants can analyze your current infrastructure and help you develop a plan to incorporate all the software and services of Microsoft 365 for enterprise.

- Do it yourself

Start with the [Networking roadmap](#) to build out or verify your existing infrastructure and productivity workloads.

For an example of how a fictional but representative multinational organization has deployed Microsoft 365 for enterprise, see the [Contoso Corporation case study](#).

Additional Microsoft 365 products

- [Microsoft 365 Business Premium](#)

Bring together the best-in-class productivity and collaboration capabilities with device management and security solutions to safeguard business data for small and midsize businesses.

- [Microsoft 365 Education](#)

Empower educators to unlock creativity, promote teamwork, and provide a simple and safe experience in a single, affordable solution built for education.

- [Microsoft 365 Government](#)

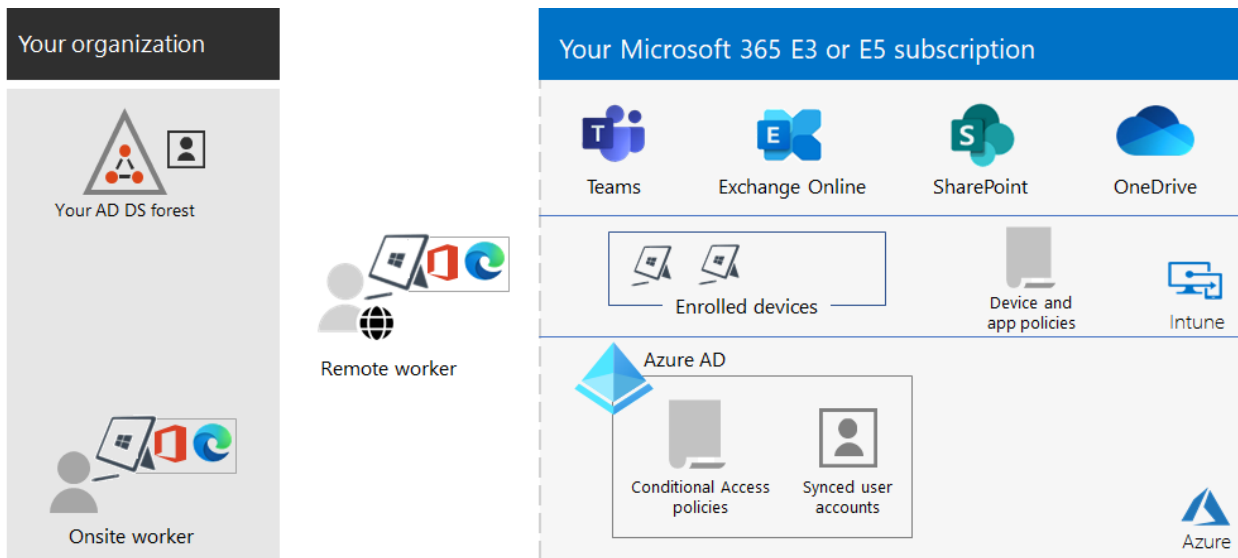
Empower United States public sector employees to work together, securely.

Best together with Surface and the Edge browser

Optimize your user's integrated and secure productivity with the best-together combination of Microsoft 365 for enterprise, Microsoft Surface devices, and the Microsoft Edge browser. This cross-product integration provides:

- A common identity and sign-in security infrastructure.
- Integrated local and cloud apps for search, collaboration, productivity, and compliance.
- Comprehensive and integrated security for hardware, browser, local app, and cloud apps.
- A common infrastructure for IT management of installs and updates.

Here is an example for an enterprise organization.



For more information and configuration examples for a small and medium business and an educational institution, download the [Best together poster](#).

Best together with Microsoft 365, Surface, and Edge

To optimize your user's productivity with integration and comprehensive security, the best-together combination is Microsoft 365 with Microsoft Surface laptops and the Microsoft Edge browser.

Microsoft 365	Surface laptop	Edge browser	Microsoft Endpoint Manager (for enterprises)
Achieve more with innovative Office apps, intelligent cloud services, search, and comprehensive support for security and compliance.	Cloud productivity apps, Microsoft 365 Apps, and enterprise-ready security and compliance features.	World-class performance and compatibility, privacy protection and control over your data, customizability for browsing, enterprise search, and personal productivity.	Endpoint security, device management and intelligent cloud services in a unified management platform.

Microsoft product suite integration	Benefits
Common identity and sign-in security	Azure Active Directory (Azure AD) is the identity provider for device and cloud apps and can enforce strong sign-in requirements with Conditional Access and multi-factor authentication (MFA).
Integrated local and cloud apps for search, collaboration, productivity and compliance	Microsoft 365 Apps is the always up-to-date suite of desktop apps you already know (including Word, PowerPoint, Excel, Outlook, and Teams) that are designed to work with Microsoft 365 cloud apps such as SharePoint, OneDrive, Exchange, and Teams.
Comprehensive and integrated security for hardware, browser, local apps, and cloud apps	World-class security is built-in to Surface laptops, Windows 10, Microsoft 365, and Edge in a way that works best together, leveraging the intelligence of the Microsoft cloud, and is transparent to users.
IT management of installs and updates	Endpoint Manager uses on-premises Configuration Manager servers and cloud-based Microsoft Intune to ensure that Windows 10, Microsoft 365 Apps, and Edge are easily installed and kept current with ongoing updates.

The following sections show the components and configurations for an enterprise, a small or medium-sized business, and an educational institution.

An enterprise organization

Your organization

Your AD DS forest

On-premise worker

Remote worker

Your Microsoft 365 E3 or E5 subscription

Teams

Exchange Online

SharePoint

OneDrive

Enrolled devices

Device and app policies

Intune

Azure AD

Conditional Access policies

User accounts

Azure

Component	That includes
Microsoft 365 E3 or E5	Cloud productivity apps, Microsoft 365 Apps, and enterprise-ready security and compliance features.
On-premise and remote worker devices	Surface laptop with Microsoft 365 Apps and the Edge browser installed.
Identity	Hybrid identity with synchronized on-premises accounts, Conditional Access policies, and MFA for secure sign-ins.
Installs and updates	On-premises network has Endpoint Configuration Manager for installs, updates, and settings.
Device management	Surface laptops are enrolled in Intune and receive device and app policies.

January 2021 © 2021 Microsoft Corporation. All rights reserved.

Best together with Microsoft 365, Surface, and Edge

A small or medium-sized business

Your business

On-premise worker

Remote worker

Your Microsoft 365 Business Premium subscription

Teams

Exchange Online

SharePoint

OneDrive

Enrolled devices

Device and app policies

Intune

Azure AD

Conditional Access policies

User accounts

Azure

Component	That includes
Microsoft 365 Business Premium	Cloud productivity apps, Microsoft 365 Apps, search, and security and compliance features.
On-premise and remote worker devices	Surface laptop with Microsoft 365 Apps and the Edge browser installed.
Identity	Cloud-only identity, Conditional Access policies, and MFA for secure sign-ins.
Installs and updates	Microsoft cloud and Intune for installs, updates, and settings.
Device management	Surface laptops are enrolled in Intune and receive device and app policies.

An educational institution

Your school's Microsoft 365 Education A3 or A5 subscription

Teams

Exchange Online

SharePoint

OneDrive

Enrolled devices

Device and app policies

Intune for Education

Azure AD

Conditional Access policies

User accounts

Azure

Component	That includes
Microsoft 365 Education A3 or A5	Cloud productivity apps, Microsoft 365 Apps, and security and compliance features.
Student devices	Surface laptop with Microsoft 365 Apps and the Edge browser installed.
Identity	Cloud-only identity, Conditional Access policies, and MFA for secure sign-ins.
Installs and updates	Microsoft cloud and Intune for Education for installs, updates, and settings.
Device management	Surface laptops are enrolled in Intune for Education and receive device and app policies.

Where to start

Microsoft 365	Surface laptops	Edge browser	Endpoint Manager
microsoft.com/microsoft365	microsoft.com/surface	microsoft.com/edge	microsoft.com/endpointmanager

January 2021 © 2021 Microsoft Corporation. All rights reserved.

Microsoft 365 training

To learn more about Microsoft 365 and work toward a Microsoft 365 certification, you can start with [Microsoft 365 Certified: Fundamentals](#).

See also

[Microsoft 365 for enterprise product page](#)

Networking roadmap for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

Microsoft 365 for enterprise includes collaboration and productivity cloud services, Microsoft Intune, and many identity and security services of Microsoft Azure. All of these cloud-based services rely on the security, performance, and reliability of connections from client devices over the Internet or dedicated circuits. To host these services and make them available to customers all over the world, Microsoft has designed a networking infrastructure that emphasizes performance and integration.

A crucial part of your Microsoft 365 onboarding is to ensure that your network and Internet connections are set up for optimized access. Configuring your on-premises network to access a globally distributed Software-as-a-Service (SaaS) cloud is different from a traditional network that is optimized for traffic to on-premises datacenters and a central Internet connection.

Use these articles to understand the key differences and to modify your edge devices, client computers, and on-premises network to get the best performance for your on-premises users.

Plan

In the planning phase of your networking implementation:

- [Understand how Microsoft 365 networking works](#)
- [Learn about network connectivity principles](#)
- [Assess your current network connectivity](#)
- [Determine if ExpressRoute is right for your organization](#)
- [Plan for your network devices](#)
- [Get your network set up for migration](#)

Deploy

In the deployment phase of your networking implementation:

- [Ensure your enterprise network is optimized for Microsoft 365 connectivity](#)
- [Add the DNS domains for your organization](#)
- [Optimize connectivity for remote workers using VPN split tunneling](#)
- [Configure CDN to improve network performance](#)
- [Optimize your connectivity to Microsoft 365 endpoints](#)
- If needed, [configure ExpressRoute](#)

Manage

In the management phase of your networking implementation:

- [Test and optimize using the Microsoft 365 network connectivity test tool](#)
- [Ensure that your network devices are using the latest Office 365 endpoints](#)
- [Monitor and tune your networking performance](#)
- [Monitor your Microsoft 365 connectivity](#)

Network equipment vendors

If you are a network equipment vendor, join the [Microsoft 365 Networking Partner Program](#). Enroll in the program to build Microsoft 365 network connectivity principles into your products and solutions.

How Contoso did networking for Microsoft 365

See how the Contoso Corporation, a fictional but representative multi-national business, [optimized their network devices and Internet connections](#) for Microsoft 365 cloud services.



Next step

Start your networking planning with the [Microsoft 365 networking connectivity overview](#).

Microsoft 365 network connectivity overview

10/28/2022 • 6 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 is a distributed Software-as-a-Service (SaaS) cloud that provides productivity and collaboration scenarios through a diverse set of micro-services and applications. Client components of Microsoft 365 such as Outlook, Word, and PowerPoint run on user computers and connect to other components of Microsoft 365 that run in Microsoft datacenters. The most significant factor that determines the quality of the Microsoft 365 end user experience is network reliability and low latency between Microsoft 365 clients and Microsoft 365 service front doors.

In this article, you will learn about the goals of Microsoft 365 networking, and why Microsoft 365 networking requires a different approach to optimization than generic Internet traffic.

Microsoft 365 networking goals

The ultimate goal of Microsoft 365 networking is to optimize the end user experience by enabling the least restrictive access between clients and the closest Microsoft 365 endpoints. The quality of end user experience is directly related to the performance and responsiveness of the application that the user is using. For example, Microsoft Teams relies on low latency so that user phone calls, conferences and shared screen collaborations are glitch-free, and Outlook relies on great networking connectivity for instant search features that apply server-side indexing and AI capabilities.

The primary goal in the network design should be to minimize latency by reducing the round-trip time (RTT) from client machines to the Microsoft Global Network, Microsoft's public network backbone that interconnects all of Microsoft's datacenters with low latency, high availability cloud application entry points spread around the world. You can learn more about the Microsoft Global Network at [How Microsoft builds its fast and reliable global network](#).

Optimizing Microsoft 365 network performance doesn't need to be complicated. You can get the best possible performance by following a few key principles:

- Identify Microsoft 365 network traffic
- Allow local branch egress of Microsoft 365 network traffic to the internet from each location where users connect to Microsoft 365
- Allow Microsoft 365 traffic to bypass proxies and packet inspection devices

For more information on Microsoft 365 network connectivity principles, see [Microsoft 365 Network Connectivity Principles](#).

Traditional network architectures and SaaS

Traditional network architecture principles for client/server workloads are designed around the assumption that traffic between clients and endpoints does not extend outside the corporate network perimeter. Also, in many enterprise networks, all outbound Internet connections traverse the corporate network, and egress from a central location.

In traditional network architectures, higher latency for generic Internet traffic is a necessary tradeoff in order to maintain network perimeter security, and performance optimization for Internet traffic typically involves upgrading or scaling out the equipment at network egress points. However, this approach does not address the requirements for optimum network performance of SaaS services such as Microsoft 365.

Identifying Microsoft 365 network traffic

We're making it easier to identify Microsoft 365 network traffic and making it simpler to manage the network identification.

- New categories of network endpoints to differentiate highly critical network traffic from network traffic that's not impacted by Internet latencies. There are just a handful of URLs and supporting IP Addresses in the most critical "Optimize" category.
- Web services for script usage or direct device configuration and change management of Microsoft 365 network identification. Changes are available from the web service, or in RSS format, or on email using a Microsoft Flow template.
- [Office 365 Network partner program](#) with Microsoft partners who provide devices or services that follow Microsoft 365 network connectivity principles and have simple configuration.

Securing Microsoft 365 connections

The goal of traditional network security is to harden the corporate network perimeter against intrusion and malicious exploits. Most enterprise networks enforce network security for Internet traffic using technologies like proxy servers, firewalls, SSL break and inspect, deep packet inspection, and data loss prevention systems. These technologies provide important risk mitigation for generic Internet requests but can dramatically reduce performance, scalability, and the quality of end user experience when applied to Microsoft 365 endpoints.

Microsoft 365 helps meet your organization's needs for content security and data usage compliance with built-in security and governance features designed specifically for Microsoft 365 features and workloads. For more information about Microsoft 365 security and compliance, see the [Office 365 security roadmap](#). For more information about Microsoft's recommendations and support position on advanced network solutions that perform advanced-level processing on Microsoft 365 traffic, see [Using third-party network devices or solutions on Office 365 traffic](#).

Why is Microsoft 365 networking different?

Microsoft 365 is designed for optimal performance using endpoint security and encrypted network connections, reducing the need for perimeter security enforcement. Microsoft 365 datacenters are located across the world and the service is designed to use various methods for connecting clients to best available service endpoints. Since user data and processing are distributed between many Microsoft datacenters, there is no single network endpoint to which client machines can connect. In fact, data and services in your Microsoft 365 tenant are dynamically optimized by the Microsoft Global Network to adapt to the geographic locations from which they are accessed by end users.

Certain common performance issues are created when Microsoft 365 traffic is subject to packet inspection and centralized egress:

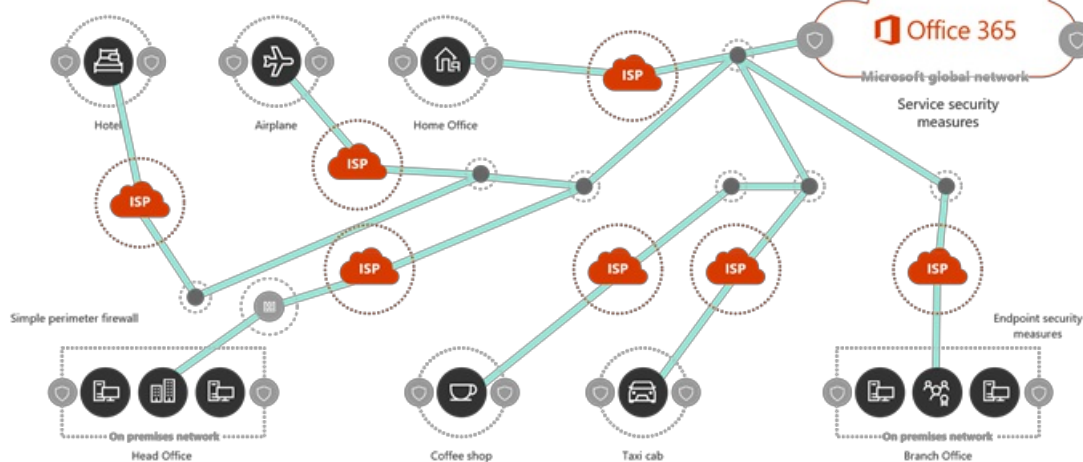
- High latency can cause poor performance of video and audio streams, and slow response of data retrieval, searches, real-time collaboration, calendar free/busy information, in-product content and other services
- Egressing connections from a central location defeats the dynamic routing capabilities of the Microsoft 365 global network, adding latency and round-trip time
- Decrypting SSL secured Microsoft 365 network traffic and re-encrypting it can cause protocol errors and has security risk

Shortening the network path to Microsoft 365 entry points by allowing client traffic to egress as close as possible to their geographic location can improve connectivity performance and the end user experience in Microsoft 365. It can also help to reduce the impact of future changes to the network architecture on Microsoft 365 performance and reliability. The optimum connectivity model is to always provide network egress at the

user's location, regardless of whether this is on the corporate network or remote locations such as home, hotels, coffee shops, and airports. Generic Internet traffic and WAN based corporate network traffic would be separately routed and not use the local direct egress model. This local direct egress model is represented in the diagram below.

Local egress direct internet network architecture

Optimal for SaaS



The local egress architecture has the following benefits for Microsoft 365 network traffic over the traditional model:

- Provides optimal Microsoft 365 performance by optimizing route length. End user connections are dynamically routed to the nearest Microsoft 365 entry point by the Microsoft Global Network's *Distributed Service Front Door* infrastructure, and traffic is then routed internally to data and service endpoints over Microsoft's ultra-low latency high availability fiber.
- Reduces the load on corporate network infrastructure by allowing local egress for Microsoft 365 traffic, bypassing proxies and traffic inspection devices.
- Secures connections on both ends by applying client endpoint security and cloud security features, avoiding application of redundant network security technologies.

NOTE

The *Distributed Service Front Door* infrastructure is the Microsoft Global Network's highly available and scalable network edge with geographically distributed locations. It terminates end user connections and efficiently routes them within the Microsoft Global Network. You can learn more about the Microsoft Global Network at [How Microsoft builds its fast and reliable global network](#).

For more information on understanding and applying Microsoft 365 network connectivity principles, see [Microsoft 365 Network Connectivity Principles](#).

Conclusion

Optimizing Microsoft 365 network performance really comes down to removing unnecessary impediments. By treating Microsoft 365 connections as trusted traffic, you can prevent latency from being introduced by packet inspection and competition for proxy bandwidth. Allowing local connections between client machines and Office 365 endpoints enables traffic to be dynamically routed through the Microsoft Global Network.

Related Topics

[Microsoft 365 Network Connectivity Principles](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning and performance tuning for Microsoft 365](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Content Delivery Networks](#)

[Microsoft 365 connectivity test](#)

[How Microsoft builds its fast and reliable global network](#)

[Office 365 Networking blog](#)

Microsoft 365 network connectivity principles

10/28/2022 • 20 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Before you begin planning your network for Microsoft 365 network connectivity, it is important to understand the connectivity principles for securely managing Microsoft 365 traffic and getting the best possible performance. This article will help you understand the most recent guidance for securely optimizing Microsoft 365 network connectivity.

Traditional enterprise networks are designed primarily to provide users access to applications and data hosted in company operated datacenters with strong perimeter security. The traditional model assumes that users will access applications and data from inside the corporate network perimeter, over WAN links from branch offices, or remotely over VPN connections.

Adoption of SaaS applications like Microsoft 365 moves some combination of services and data outside the network perimeter. Without optimization, traffic between users and SaaS applications is subject to latency introduced by packet inspection, network hairpins, inadvertent connections to geographically distant endpoints and other factors. You can ensure the best Microsoft 365 performance and reliability by understanding and implementing key optimization guidelines.

In this article, you will learn about:

- [Microsoft 365 architecture](#) as it applies to customer connectivity to the cloud
- Updated [Microsoft 365 connectivity principles](#) and strategies for optimizing network traffic and the end-user experience
- The [Office 365 Endpoints web service](#), which allows network administrators to consume a structured list of endpoints for use in network optimization
- [New Office 365 endpoint categories](#) and optimization guidance
- [Comparing network perimeter security with endpoint security](#)
- [Incremental optimization](#) options for Microsoft 365 traffic
- The [Microsoft 365 connectivity test](#), a new tool for testing basic connectivity to Microsoft 365

Microsoft 365 architecture

Microsoft 365 is a distributed Software-as-a-Service (SaaS) cloud that provides productivity and collaboration scenarios through a diverse set of micro-services and applications, such as Exchange Online, SharePoint Online, Skype for Business Online, Microsoft Teams, Exchange Online Protection, Office in a browser, and many others. While specific Microsoft 365 applications may have their unique features as it applies to customer network and connectivity to the cloud, they all share some key principals, goals, and architecture patterns. These principles and architecture patterns for connectivity are typical for many other SaaS clouds and at the same time being different from the typical deployment models of Platform-as-a-Service and Infrastructure-as-a-Service clouds, such as Microsoft Azure.

One of the most significant architectural features of Microsoft 365 (that is often missed or misinterpreted by network architects) is that it is a truly global distributed service, in the context of how users connect to it. The location of the target Microsoft 365 tenant is important to understand the locality of where customer data is stored within the cloud, but the user experience with Microsoft 365 doesn't involve connecting directly to disks containing the data. The user experience with Microsoft 365 (including performance, reliability, and other important quality characteristics) involves connectivity through highly distributed service front doors that are

scaled out across hundreds of Microsoft locations worldwide. In the majority of cases, the best user experience is achieved by allowing the customer network to route user requests to the closest Microsoft 365 service entry point, rather than connecting to Microsoft 365 through an egress point in a central location or region.

For most customers, Microsoft 365 users are distributed across many locations. To achieve the best results, the principles outlined in this document should be looked at from the scale-out (not scale-up) point of view, focusing on optimizing connectivity to the nearest point of presence in the Microsoft Global Network, not to the geographic location of the Microsoft 365 tenant. In essence, this means that even though Microsoft 365 tenant data may be stored in a specific geographic location, Microsoft 365 experience for that tenant remains distributed, and can be present in very close (network) proximity to every end-user location that the tenant has.

Microsoft 365 connectivity principles

Microsoft recommends the following principles to achieve optimal Microsoft 365 connectivity and performance. Use these Microsoft 365 connectivity principles to manage your traffic and get the best performance when connecting to Microsoft 365.

The primary goal in the network design should be to minimize latency by reducing the round-trip time (RTT) from your network into the Microsoft Global Network, Microsoft's public network backbone that interconnects all of Microsoft's datacenters with low latency and cloud application entry points spread around the world. You can learn more about the Microsoft Global Network at [How Microsoft builds its fast and reliable global network](#).

Identify and differentiate Microsoft 365 traffic



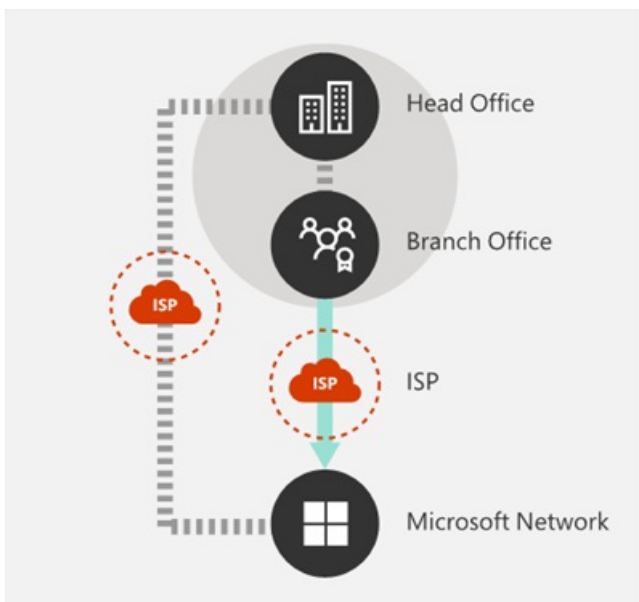
Identifying Microsoft 365 network traffic is the first step in being able to differentiate that traffic from generic Internet-bound network traffic. Microsoft 365 connectivity can be optimized by implementing a combination of approaches like network route optimization, firewall rules, browser proxy settings, and bypass of network inspection devices for certain endpoints.

Previous Microsoft 365 optimization guidance divided Microsoft 365 endpoints into two categories, **Required** and **Optional**. As endpoints have been added to support new Microsoft 365 services and features, we have reorganized Microsoft 365 endpoints into three categories: **Optimize**, **Allow**, and **Default**. Guidelines for each category applies to all endpoints in the category, making optimizations easier to understand and implement.

For more information on Microsoft 365 endpoint categories and optimization methods, see the [New Office 365 endpoint categories](#) section.

Microsoft now publishes all Microsoft 365 endpoints as a web service and provides guidance on how best to use this data. For more information on how to fetch and work with Microsoft 365 endpoints, see the article [Office 365 URLs and IP address ranges](#).

Egress network connections locally



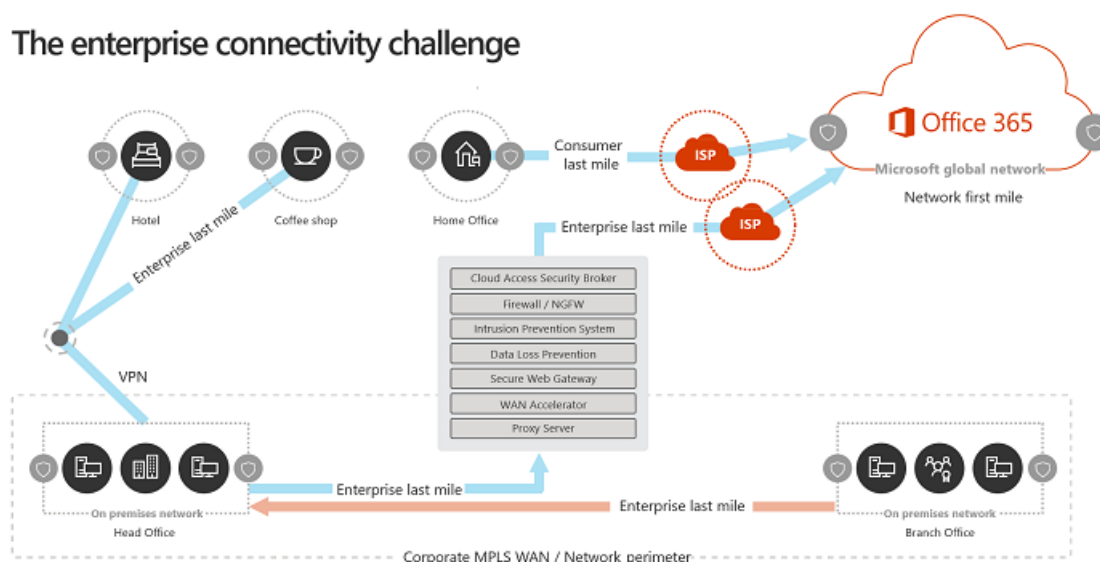
Local DNS and Internet egress is of critical importance for reducing connection latency and ensuring that user connections are made to the nearest point of entry to Microsoft 365 services. In a complex network topology, it is important to implement both local DNS and local Internet egress together. For more information about how Microsoft 365 routes client connections to the nearest point of entry, see the article [Client Connectivity](#).

Prior to the advent of cloud services such as Microsoft 365, end-user Internet connectivity as a design factor in network architecture was relatively simple. When Internet services and web sites are distributed around the globe, latency between corporate egress points and any given destination endpoint is largely a function of geographical distance.

In a traditional network architecture, all outbound Internet connections traverse the corporate network, and egress from a central location. As Microsoft's cloud offerings have matured, a distributed Internet-facing network architecture has become critical for supporting latency-sensitive cloud services. The Microsoft Global Network was designed to accommodate latency requirements with the Distributed Service Front Door infrastructure, a dynamic fabric of global entry points that routes incoming cloud service connections to the closest entry point. This is intended to reduce the length of the "last mile" for Microsoft cloud customers by effectively shortening the route between the customer and the cloud.

Enterprise WANs are often designed to backhaul network traffic to a central company head office for inspection before egress to the Internet, usually through one or more proxy servers. The diagram below illustrates such a network topology.

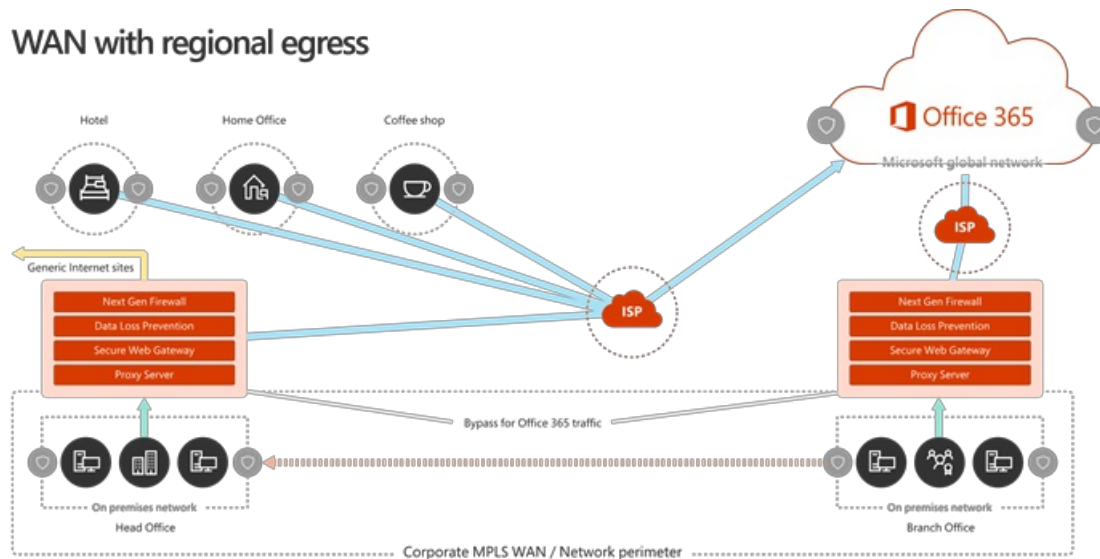
The enterprise connectivity challenge



Because Microsoft 365 runs on the Microsoft Global Network, which includes front-end servers around the

world, there will often be a front-end server close to the user's location. By providing local Internet egress and by configuring internal DNS servers to provide local name resolution for Microsoft 365 endpoints, network traffic destined for Microsoft 365 can connect to Microsoft 365 front end servers as close as possible to the user. The diagram below shows an example of a network topology that allows users connecting from main office, branch office, and remote locations to follow the shortest route to the closest Microsoft 365 entry point.

WAN with regional egress



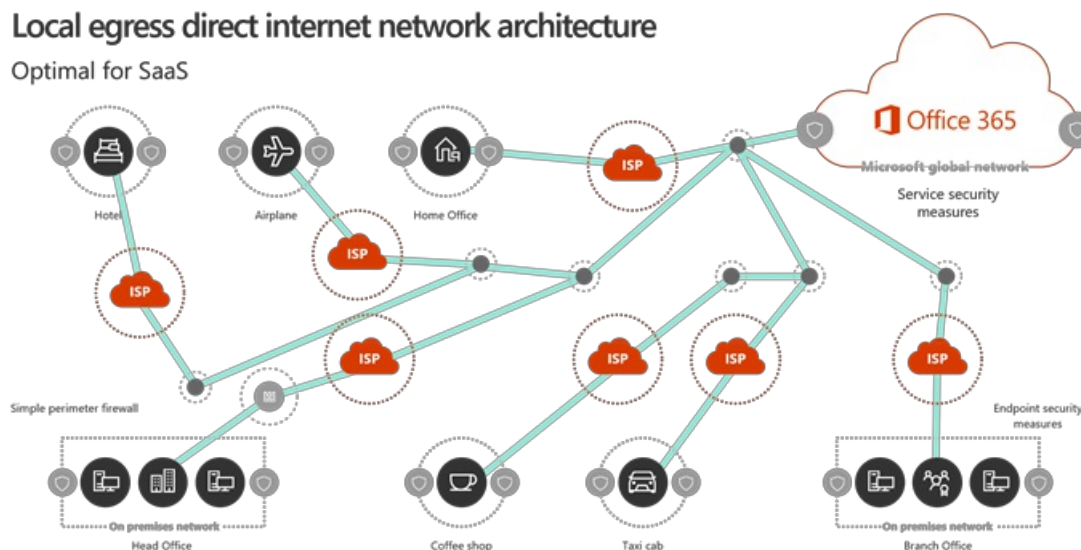
Shortening the network path to Microsoft 365 entry points in this way can improve connectivity performance and the end-user experience in Microsoft 365, and can also help to reduce the impact of future changes to the network architecture on Microsoft 365 performance and reliability.

Also, DNS requests can introduce latency if the responding DNS server is distant or busy. You can minimize name resolution latency by provisioning local DNS servers in branch locations and making sure they are configured to cache DNS records appropriately.

While regional egress can work well for Microsoft 365, the optimum connectivity model would be to always provide network egress at the user's location, regardless of whether this is on the corporate network or remote locations such as homes, hotels, coffee shops, and airports. This local direct egress model is represented in the diagram below.

Local egress direct internet network architecture

Optimal for SaaS

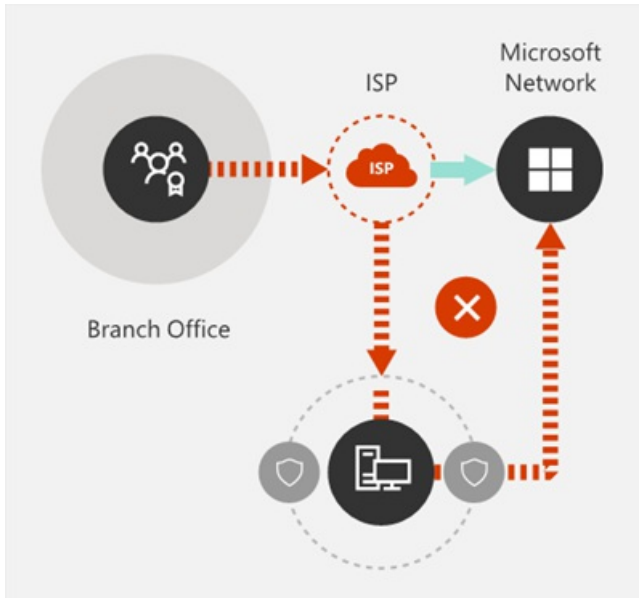


Enterprises who have adopted Microsoft 365 can take advantage of the Microsoft Global Network's Distributed Service Front Door architecture by ensuring that user connections to Microsoft 365 take the shortest possible route to the nearest Microsoft Global Network entry point. The local egress network architecture does this by allowing Microsoft 365 traffic to be routed over the nearest egress, regardless of user location.

The local egress architecture has the following benefits over the traditional model:

- Provides optimal Microsoft 365 performance by optimizing route length. end-user connections are dynamically routed to the nearest Microsoft 365 entry point by the Distributed Service Front Door infrastructure.
- Reduces the load on corporate network infrastructure by allowing local egress.
- Secures connections on both ends by leveraging client endpoint security and cloud security features.

Avoid network hairpins



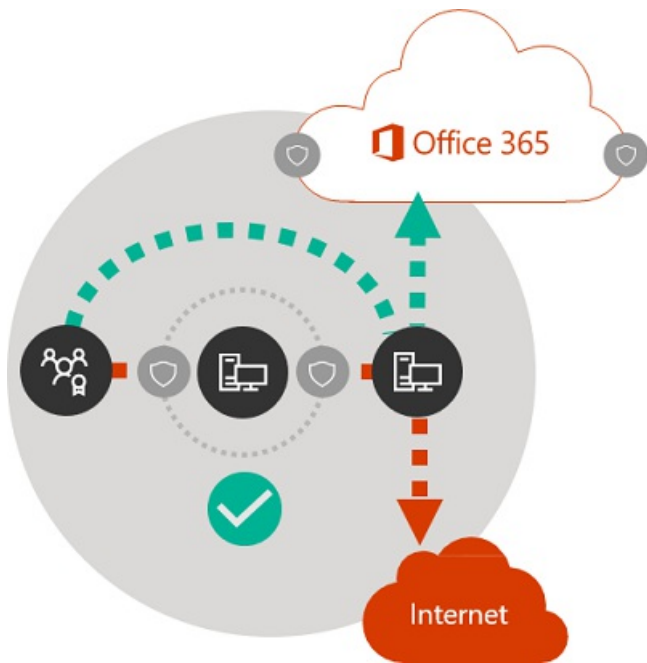
As a general rule of thumb, the shortest, most direct route between user and closest Microsoft 365 endpoint will offer the best performance. A network hairpin happens when WAN or VPN traffic bound for a particular destination is first directed to another intermediate location (such as security stack, cloud access broker, or cloud-based web gateway), introducing latency and potential redirection to a geographically distant endpoint. Network hairpins can also be caused by routing/peering inefficiencies or suboptimal (remote) DNS lookups.

To ensure that Microsoft 365 connectivity is not subject to network hairpins even in the local egress case, check whether the ISP that is used to provide Internet egress for the user location has a direct peering relationship with the Microsoft Global Network in close proximity to that location. You may also want to configure egress routing to send trusted Microsoft 365 traffic directly, as opposed to proxying or tunneling through a third-party cloud or cloud-based network security vendor that processes your Internet-bound traffic. Local DNS name resolution of Microsoft 365 endpoints helps to ensure that in addition to direct routing, the closest Microsoft 365 entry points are being used for user connections.

If you use cloud-based network or security services for your Microsoft 365 traffic, ensure that the result of the hairpin is evaluated and its impact on Microsoft 365 performance is understood. This can be done by examining the number and locations of service provider locations through which the traffic is forwarded in relationship to number of your branch offices and Microsoft Global Network peering points, quality of the network peering relationship of the service provider with your ISP and Microsoft, and the performance impact of backhauling in the service provider infrastructure.

Due to the large number of distributed locations with Microsoft 365 entry points and their proximity to end-users, routing Microsoft 365 traffic to any third-party network or security provider can have an adverse impact on Microsoft 365 connections if the provider network is not configured for optimal Microsoft 365 peering.

Assess bypassing proxies, traffic inspection devices, and duplicate security technologies



Enterprise customers should review their network security and risk reduction methods specifically for Microsoft 365 bound traffic and use Microsoft 365 security features to reduce their reliance on intrusive, performance impacting, and expensive network security technologies for Microsoft 365 network traffic.

Most enterprise networks enforce network security for Internet traffic using technologies like proxies, SSL inspection, packet inspection, and data loss prevention systems. These technologies provide important risk mitigation for generic Internet requests but can dramatically reduce performance, scalability, and the quality of end user experience when applied to Microsoft 365 endpoints.

Office 365 Endpoints web service

Microsoft 365 administrators can use a script or REST call to consume a structured list of endpoints from the Office 365 Endpoints web service and update the configurations of perimeter firewalls and other network devices. This will ensure that traffic bound for Microsoft 365 is identified, treated appropriately and managed differently from network traffic bound for generic and often unknown Internet web sites. For more information on how to use the Office 365 Endpoints web service, see the article [Office 365 URLs and IP address ranges](#).

PAC (Proxy Automatic Configuration) scripts

Microsoft 365 administrators can create PAC (Proxy Automatic Configuration) scripts that can be delivered to user computers via WPAD or GPO. PAC scripts can be used to bypass proxies for Microsoft 365 requests from WAN or VPN users, allowing Microsoft 365 traffic to use direct Internet connections rather than traversing the corporate network.

Microsoft 365 security features

Microsoft is transparent about datacenter security, operational security, and risk reduction around Microsoft 365 servers and the network endpoints that they represent. Microsoft 365 built-in security features are available for reducing network security risk, such as Microsoft Purview Data Loss Prevention, Anti-Virus, Multi-Factor Authentication, Customer Lock Box, Defender for Office 365, Microsoft 365 Threat Intelligence, Microsoft 365 Secure Score, Exchange Online Protection, and Network DDOS Security.

For more information on Microsoft datacenter and Global Network security, see the [Microsoft Trust Center](#).

New Office 365 endpoint categories

Office 365 endpoints represent a varied set of network addresses and subnets. Endpoints may be URLs, IP addresses or IP ranges, and some endpoints are listed with specific TCP/UDP ports. URLs can either be an FQDN

like *account.office.net*, or a wildcard URL like **.office365.com*.

NOTE

The locations of Office 365 endpoints within the network are not directly related to the location of the Microsoft 365 tenant data. For this reason, customers should look at Microsoft 365 as a distributed and global service and should not attempt to block network connections to Office 365 endpoints based on geographical criteria.

In our previous guidance for managing Microsoft 365 traffic, endpoints were organized into two categories, **Required** and **Optional**. Endpoints within each category required different optimizations depending on the criticality of the service, and many customers faced challenges in justifying the application of the same network optimizations to the full list of Office 365 URLs and IP addresses.

In the new model, endpoints are segregated into three categories, **Optimize**, **Allow**, and **Default**, providing a priority-based pivot on where to focus network optimization efforts to realize the best performance improvements and return on investment. The endpoints are consolidated in the above categories based on the sensitivity of the effective user experience to network quality, volume, and performance envelope of scenarios and ease of implementation. Recommended optimizations can be applied the same way to all endpoints in a given category.

- **Optimize** endpoints are required for connectivity to every Office 365 service and represent over 75% of Office 365 bandwidth, connections, and volume of data. These endpoints represent Office 365 scenarios that are the most sensitive to network performance, latency, and availability. All endpoints are hosted in Microsoft datacenters. The rate of change to the endpoints in this category is expected to be much lower than for the endpoints in the other two categories. This category includes a small (on the order of ~10) set of key URLs and a defined set of IP subnets dedicated to core Office 365 workloads such as Exchange Online, SharePoint Online, Skype for Business Online, and Microsoft Teams.

A condensed list of well-defined critical endpoints should help you to plan and implement high value network optimizations for these destinations faster and easier.

Examples of *Optimize* endpoints include <https://outlook.office365.com>, <https://<tenant>.sharepoint.com>, and <https://<tenant>-my.sharepoint.com>.

Optimization methods include:

- Bypass *Optimize* endpoints on network devices and services that perform traffic interception, SSL decryption, deep packet inspection, and content filtering.
 - Bypass on-premises proxy devices and cloud-based proxy services commonly used for generic Internet browsing.
 - Prioritize the evaluation of these endpoints as fully trusted by your network infrastructure and perimeter systems.
 - Prioritize reduction or elimination of WAN backhauling, and facilitate direct distributed Internet-based egress for these endpoints as close to users/branch locations as possible.
 - Facilitate direct connectivity to these cloud endpoints for VPN users by implementing split tunneling.
 - Ensure that IP addresses returned by DNS name resolution match the routing egress path for these endpoints.
 - Prioritize these endpoints for SD-WAN integration for direct, minimal latency routing into the nearest Internet peering point of the Microsoft global network.
- **Allow** endpoints are required for connectivity to specific Office 365 services and features, but are not as sensitive to network performance and latency as those in the *Optimize* category. The overall network footprint of these endpoints from the standpoint of bandwidth and connection count is also smaller. These endpoints are dedicated to Office 365 and are hosted in Microsoft datacenters. They represent a broad set of Office 365 micro-services and their dependencies (on the order of ~100 URLs) and are

expected to change at a higher rate than those in the *Optimize* category. Not all endpoints in this category are associated with defined dedicated IP subnets.

Network optimizations for *Allow* endpoints can improve the Office 365 user experience, but some customers may choose to scope those optimizations more narrowly to minimize changes to their network.

Examples of *Allow* endpoints include https://*.protection.outlook.com and <https://accounts.accesscontrol.windows.net>.

Optimization methods include:

- Bypass *Allow* endpoints on network devices and services that perform traffic interception, SSL decryption, deep packet inspection, and content filtering.
- Prioritize the evaluation of these endpoints as fully trusted by your network infrastructure and perimeter systems.
- Prioritize reduction or elimination of WAN backhauling, and facilitate direct distributed Internet-based egress for these endpoints as close to users/branch locations as possible.
- Ensure that IP addresses returned by DNS name resolution match the routing egress path for these endpoints.
- Prioritize these endpoints for SD-WAN integration for direct, minimal latency routing into the nearest Internet peering point of the Microsoft global network.
- **Default** endpoints represent Office 365 services and dependencies that do not require any optimization, and can be treated by customer networks as normal Internet bound traffic. Some endpoints in this category may not be hosted in Microsoft datacenters. Examples include <https://odc.officeapps.live.com> and <https://appexsin.stb.s-msn.com>.

For more information about Office 365 network optimization techniques, see the article [Managing Office 365 endpoints](#).

Comparing network perimeter security with endpoint security

The goal of traditional network security is to harden the corporate network perimeter against intrusion and malicious exploits. As organizations adopt Microsoft 365, some network services and data are partly or completely migrated to the cloud. As for any fundamental change to network architecture, this process requires a reevaluation of network security that takes emerging factors into account:

- As cloud services are adopted, network services and data are distributed between on-premises datacenters and the cloud, and perimeter security is no longer adequate on its own.
- Remote users connect to corporate resources both in on-premises datacenters and in the cloud from uncontrolled locations such as homes, hotels, and coffee shops.
- Purpose-built security features are increasingly built into cloud services and can potentially supplement or replace existing security systems.

Microsoft offers a wide range of Microsoft 365 security features and provides prescriptive guidance for employing security best practices that can help you to ensure data and network security for Microsoft 365. Recommended best practices include the following:

- **Use multi-factor authentication (MFA)** MFA adds an additional layer of protection to a strong password strategy by requiring users to acknowledge a phone call, text message, or an app notification on their smart phone after correctly entering their password.
- **Use Microsoft Defender for Cloud Apps** Configure policies to track anomalous activity and act on it. Set up alerts with Microsoft Defender for Cloud Apps so that admins can review unusual or risky user activity, such as downloading large amounts of data, multiple failed sign-in attempts, or connections from

a unknown or dangerous IP addresses.

- **Configure Data Loss Prevention (DLP)** DLP allows you to identify sensitive data and create policies that help prevent your users from accidentally or intentionally sharing the data. DLP works across Microsoft 365 including Exchange Online, SharePoint Online, and OneDrive so that your users can stay compliant without interrupting their workflow.
- **Use Customer Lockbox** As a Microsoft 365 admin, you can use Customer Lockbox to control how a Microsoft support engineer accesses your data during a help session. In cases where the engineer requires access to your data to troubleshoot and fix an issue, Customer Lockbox allows you to approve or reject the access request.
- **Use Office 365 Secure Score** A security analytics tool that recommends what you can do to further reduce risk. Secure Score looks at your Microsoft 365 settings and activities and compares them to a baseline established by Microsoft. You'll get a score based on how aligned you are with best security practices.

A holistic approach to enhanced security should include consideration of the following:

- Shift emphasis from perimeter security towards endpoint security by applying cloud-based and Office client security features.
 - Shrink the security perimeter to the datacenter
 - Enable equivalent trust for user devices inside the office or at remote locations
 - Focus on securing the data location and the user location
 - Managed user machines have higher trust with endpoint security
- Manage all information security holistically, not focusing solely on the perimeter
 - Redefine WAN and building perimeter network security by allowing trusted traffic to bypass security devices and separating unmanaged devices to guest Wi-Fi networks
 - Reduce network security requirements of the corporate WAN edge
 - Some network perimeter security devices such as firewalls are still required, but load is decreased
 - Ensures local egress for Microsoft 365 traffic
- Improvements can be addressed incrementally as described in the [Incremental optimization](#) section. Some optimization techniques may offer better cost/benefit ratios depending on your network architecture, and you should choose optimizations that make the most sense for your organization.

For more information on Microsoft 365 security and compliance, see the articles [Microsoft 365 security](#) and [Microsoft Purview](#).

Incremental optimization

We have represented the ideal network connectivity model for SaaS earlier in this article, but for many large organizations with historically complex network architectures, it will not be practical to directly make all of these changes. In this section, we discuss a number of incremental changes that can help to improve Microsoft 365 performance and reliability.

The methods you will use to optimize Microsoft 365 traffic will vary depending on your network topology and the network devices you have implemented. Large enterprises with many locations and complex network security practices will need to develop a strategy that includes most or all of the principles listed in the [Microsoft 365 connectivity principles](#) section, while smaller organizations might only need to consider one or two.

You can approach optimization as an incremental process, applying each method successively. The following table lists key optimization methods in order of their impact on latency and reliability for the largest number of users.

OPTIMIZATION METHOD	DESCRIPTION	IMPACT
Local DNS resolution and Internet egress	Provision local DNS servers in each location and ensure that Microsoft 365 connections egress to the Internet as close as possible to the user's location.	Minimize latency Improve reliable connectivity to the closest Microsoft 365 entry point
Add regional egress points	If your corporate network has multiple locations but only one egress point, add regional egress points to enable users to connect to the closest Microsoft 365 entry point.	Minimize latency Improve reliable connectivity to the closest Microsoft 365 entry point
Bypass proxies and inspection devices	Configure browsers with PAC files that send Microsoft 365 requests directly to egress points. Configure edge routers and firewalls to permit Microsoft 365 traffic without inspection.	Minimize latency Reduce load on network devices
Enable direct connection for VPN users	For VPN users, enable Microsoft 365 connections to connect directly from the user's network rather than over the VPN tunnel by implementing split tunneling.	Minimize latency Improve reliable connectivity to the closest Microsoft 365 entry point
Migrate from traditional WAN to SD-WAN	SD-WANs (Software Defined Wide Area Networks) simplify WAN management and improve performance by replacing traditional WAN routers with virtual appliances, similar to the virtualization of compute resources using virtual machines (VMs).	Improve performance and manageability of WAN traffic Reduce load on network devices

Related topics

[Microsoft 365 Network Connectivity Overview](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning and performance tuning for Microsoft 365](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Content Delivery Networks](#)

[Microsoft 365 connectivity test](#)

[How Microsoft builds its fast and reliable global network](#)

[Office 365 Networking blog](#)

Assessing Microsoft 365 network connectivity

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 is designed to enable customers all over the world to connect to the service using an internet connection. As the service evolves, the security, performance, and reliability of Microsoft 365 are improved based on customers using the internet to establish a connection to the service.

Customers planning to use Microsoft 365 should assess their existing and forecasted internet connectivity needs as a part of the deployment project. For enterprise class deployments reliable and appropriately sized internet connectivity is a critical part of consuming Microsoft 365 features and scenarios.

Network evaluations can be performed by many different people and organizations depending on your size and preferences. The network scope of the assessment can also vary depending on where you're at in your deployment process. To help you get a better understanding of what it takes to perform a network assessment, we've produced a network assessment guide to help you understand the options available to you. This assessment will determine what steps and resources need to be added to the deployment project to enable you to successfully adopt Microsoft 365.

A comprehensive network assessment will provide possible solutions to networking design challenges along with implementation details. Some network assessments will show that optimal network connectivity to Microsoft 365 can be accommodated with minor configuration or design changes to the existing network and internet egress infrastructure.

Some assessments will indicate network connectivity to Microsoft 365 will require additional investments in networking components. For example, enterprise networks that span branch offices and multiple geographic regions may require investments in SD-WAN solutions or optimized routing infrastructure to support internet connectivity to Microsoft 365. Occasionally an assessment will indicate network connectivity to Microsoft 365 is influenced by regulation or performance requirements for scenarios such as [Skype for Business Online media quality](#). These additional requirements may lead to investments in internet connectivity infrastructure, routing optimization, and specialized direct connectivity.

Some resources to help you assess your network:

- See [Microsoft 365 network connectivity overview](#) for conceptual information about Microsoft 365 networking.
- See [Microsoft 365 Network Connectivity Principles](#) to understand the connectivity principles for securely managing Microsoft 365 traffic and getting the best possible performance.
- Sign up for [Microsoft FastTrack](#) for guided assistance with Microsoft 365 planning, design and deployment.
- See the [Microsoft 365 connectivity test](#) section below to run basic connectivity tests that provide specific guidance about networking connectivity improvements that can be made between a given user location and Microsoft 365.

NOTE

Microsoft authorization is required to use ExpressRoute for Office 365. Microsoft reviews every customer request and only authorizes ExpressRoute for Office 365 usage when a customer's regulatory requirement mandates direct connectivity. If you have such requirements, please provide the text excerpt and web link to the regulation which you interpret to mean that direct connectivity is required in the [ExpressRoute for Office 365 Request Form](#) to begin a Microsoft review. Unauthorized subscriptions trying to create route filters for Office 365 will receive an [error message](#).

Key points to consider when planning your network assessment for Microsoft 365:

- Microsoft 365 is a secure, reliable, high performance service that runs over the public internet. We continue to invest to enhance these aspects of the service. All Microsoft 365 services are available via internet connectivity.
- We are continually optimizing core aspects of Microsoft 365 such as availability, global reach, and performance for internet based connectivity. For example, many Microsoft 365 services leverage an expanding set of internet facing edge nodes. This edge network offers the best proximity and performance to connections coming over the internet.
- When considering using Microsoft 365 for any of the included services such as Teams or Skype for Business Online voice, video, or meeting capabilities, customers should complete an end to end network assessment and meet connectivity requirements using [Microsoft FastTrack](#).

If you're evaluating Microsoft 365 and aren't sure where to begin with your network assessment or have found network design challenges that you need assistance to overcome, please work with your Microsoft account team.

The Microsoft 365 connectivity test

The [Microsoft 365 connectivity test](#) is a proof of concept (POC) network assessment tool that runs basic connectivity tests against your Microsoft 365 tenant and makes specific network design recommendations for optimal Microsoft 365 performance. The tool highlights common large enterprise network perimeter design choices which are useful for Internet web browsing but impact the performance of large SaaS applications such as Microsoft 365.

The Network Onboarding tool does the following:

- Detects your location, or you can specify a location to test
- Checks the location of your network egress
- Tests the network path to the nearest Microsoft 365 service front door
- Provides advanced tests using a downloadable Windows 10 application that makes perimeter network design recommendations related to proxy servers, firewalls, and DNS. The tool also runs performance tests for Skype for Business Online, Microsoft Teams, SharePoint Online and Exchange Online.

The tool has two components: a browser-based UI that collects basic connectivity information, and a downloadable Windows 10 application that runs advanced tests and returns additional assessment data.

The browser-based tool displays the following information:

- Results and impact tab
 - The location on a map of the in-use service front door
 - The location on a map of other service front doors that would provide optimal connectivity
 - Relative performance compared to other Microsoft 365 customers near you
- Details and solutions tab
 - User location by city and country
 - Network egress location by city, state and country
 - User to network egress distance
 - Microsoft 365 Exchange Online service front door location
 - Optimal Microsoft 365 Exchange Online service front door(s) for user location
 - Customers in your metro area with better performance

The Advanced Tests downloadable application provides the following additional information:

- Details and solutions tab (appended)
 - User's default gateway
 - Client DNS Server
 - Client DNS Recursive Resolver
 - Exchange Online DNS server
 - SharePoint Online DNS server
 - Proxy server identification
 - Media connectivity check
 - Media quality packet loss
 - Media quality latency
 - Media quality jitter
 - Media quality packet reorder
- Connectivity tests to multiple feature-specific endpoints
- Network path diagnostics that include tracert and latency data for the Exchange Online, SharePoint Online and Teams services

You can read about the Microsoft 365 connectivity test and provide feedback at the [Updated Microsoft 365 connectivity test POC with new network design recommendations](#) blog post. Information about future updates to this tool and other Microsoft 365 networking updates will be posted to the [Office 365 Networking](#) blog.

Here's a short link you can use to come back: <https://aka.ms/o365networkconnectivity>.

Related topics

[Microsoft 365 Network Connectivity Overview](#)

[Microsoft 365 Network Connectivity Principles](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Microsoft 365 network and performance tuning](#)

[Microsoft 365 Enterprise overview](#)

Network planning with ExpressRoute for Office 365

10/28/2022 • 13 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

ExpressRoute for Office 365 provides layer 3 connectivity between your network and Microsoft's datacenters. The circuits use Border Gateway Protocol (BGP) route advertisements of Office 365's front-end servers. From the perspective of your on-premises devices, when they need to select the correct TCP/IP path to Office 365, Azure ExpressRoute is seen as an alternative to the Internet.

Azure ExpressRoute adds a direct path to a specific set of supported features and services that are offered by Office 365 servers within Microsoft's datacenters. Azure ExpressRoute doesn't replace Internet connectivity to Microsoft datacenters or basic Internet services such as domain name resolution. Azure ExpressRoute and your Internet circuits should be secured and redundant.

The following table highlights a few differences between the internet and Azure ExpressRoute connections in the context of Office 365.

DIFFERENCES IN NETWORK PLANNING	INTERNET NETWORK CONNECTION	EXPRESSROUTE NETWORK CONNECTION
Access to required internet services, including; DNS name resolution Certificate revocation verification Content Delivery Networks (CDNs)	Yes	Requests to Microsoft owned DNS and/or CDN infrastructure may use the ExpressRoute network.
Access to Office 365 services, including; Exchange Online SharePoint Online Skype for Business Online Office in a browser Office 365 Portal and Authentication	Yes, all applications and features	Yes, specific applications and features
On-premises security at perimeter.	Yes	Yes
High availability planning.	Fail over to an alternate internet network connection	Fail over to an alternate ExpressRoute connection
Direct connection with a predictable network profile.	No	Yes
IPv6 connectivity.	Yes	Yes

Expand the titles below for more network planning guidance.

Existing Azure ExpressRoute customers

If you're using an existing Azure ExpressRoute circuit and would like to add Office 365 connectivity over this circuit, you should look at the number of circuits, egress locations, and size of the circuits to ensure they'll meet the needs of your Office 365 usage. Most customers require extra bandwidth and many require more circuits.

To enable access to Office 365 over your existing Azure ExpressRoute circuits, [configure the route filters](#) to

ensure the Office 365 services are accessible.

The Azure ExpressRoute subscription is customer-centric, meaning subscriptions are tied to customers. As a customer, you can have multiple Azure ExpressRoute circuits and can access many Microsoft cloud resources over those circuits. For example, you can choose to access an Azure hosted virtual machine, an Office 365 test tenant, and an Office 365 production tenant over a pair of redundant Azure ExpressRoute circuits.

This table outlines the two types of peering relationships you can choose to implement over your circuits.

PEERING RELATIONSHIP	AZURE PRIVATE	MICROSOFT
Services	IaaS: Azure Virtual Machines	PaaS: Azure public services SaaS: Office 365 SaaS: Dynamics 365
Connection initiation	Customer-to-Microsoft Microsoft-to-Customer	Customer-to-Microsoft Microsoft-to-Customer
QoS support	No QoS	QoS ¹

¹ QoS supports Skype for Business only at this time.

Bandwidth planning for Azure ExpressRoute

Every Office 365 customer has unique bandwidth needs depending on the number of people at each location, how active they are with each Office 365 application, and other factors such as the use of on-premises or hybrid equipment and network security configurations.

Having too little bandwidth will result in congestion, retransmissions of data, and unpredictable delays. Having too much bandwidth will result in unnecessary cost. On an existing network, bandwidth is often referred to in terms of the amount of available headroom on the circuit as a percentage. Having 10% headroom will likely result in congestion and having 80% headroom generally means unnecessary cost. Typical headroom target allocations are 20% to 50%.

To find the right level of bandwidth, the best mechanism is to test your existing network consumption. This is the only way to get a true measure of usage and need as every network configuration and applications are in some ways unique. When measuring, you'll want to pay close attention to the total bandwidth consumption, latency, and TCP congestion to understand your network needs.

Once you have an estimated baseline that includes all network applications, pilot Office 365 with a small group that comprises the different profiles of people in your organization to determine actual usage, and use the two measurements to estimate the amount of bandwidth you'll require for each office location. If there are any latency or TCP congestion issues found in your testing, you may need to move the egress closer to the people using Office 365 or remove intensive network scanning such as SSL decryption/inspection.

All of our recommendations on what type of network processing is recommended applies to both ExpressRoute and Internet circuits. The same is true for the rest of the guidance on our [performance tuning site](#).

Applying security controls to Azure ExpressRoute for Office 365 scenarios

Securing Azure ExpressRoute connectivity starts with the same principles as securing Internet connectivity. Many customers choose to deploy network and perimeter controls along the ExpressRoute path connecting their on-premises network to Office 365 and other Microsoft clouds. These controls may include firewalls, application proxies, data leakage prevention, intrusion detection, intrusion prevention systems, and so on. In many cases customers apply different levels of controls to traffic initiated from on-premises going to Microsoft, versus

traffic initiated from Microsoft going to customer on-premises network, versus traffic initiated from on-premises going to a general Internet destination.

Here's a few examples of integrating security with the [ExpressRoute connectivity model](#) you choose to deploy.

EXPRESSROUTE INTEGRATION OPTION	NETWORK SECURITY PERIMETER MODEL
Colocated at a cloud exchange	Install new or use existing security/perimeter infrastructure in the colocation facility where the ExpressRoute connection is established. Use colocation facility purely for routing/interconnect purposes and back haul connections from colocation facility into the on-premises security/perimeter infrastructure.
Point-to-Point Ethernet	Terminate the Point-to-Point ExpressRoute connection in the existing on-premises security/perimeter infrastructure location. Install new security/perimeter infrastructure specific to the ExpressRoute path and terminate the Point-to-Point connection there.
Any-to-Any IPVPN	Use an existing on-premises security/perimeter infrastructure at all locations that egress into the IPVPN used for ExpressRoute for Office 365 connectivity. Hairpin the IPVPN used for ExpressRoute for Office 365 to specific on-premises locations designated to serve as the security/perimeter.

Some service providers also offer managed security/perimeter functionality as a part of their integration solutions with Azure ExpressRoute.

When considering the topology placement of the network/security perimeter options used for ExpressRoute for Office 365 connections, following are extra considerations

- The depth and type network/security controls may have impact on the performance and scalability of the Office 365 user experience.
- Outbound (on-premises->Microsoft) and inbound (Microsoft->on-premises) [if enabled] flows may have different requirements. These are likely different than Outbound to general Internet destinations.
- Office 365 requirements for ports/protocols and necessary IP subnets are the same, whether traffic is routed through ExpressRoute for Office 365 or through the Internet.
- Topological placement of the customer network/security controls determines the ultimate end to end network between the user and Office 365 service and can have a substantial impact on network latency and congestion.
- Customers are encouraged to design their security/perimeter topology for use with ExpressRoute for Office 365 in accordance with best practices for redundancy, high availability, and disaster recovery.

Here's an example of Contoso that compares the different Azure ExpressRoute connectivity options with the perimeter security models discussed above.

Example 1: Securing Azure ExpressRoute

Contoso is considering implementing Azure ExpressRoute and after planning the optimal architecture for [Routing with ExpressRoute for Office 365](#) and after using the above guidance to understand bandwidth requirements, they're determining the best method for securing their perimeter.

For Contoso, a multi-national organization with locations in multiple continents, security must span all

perimeters. The optimal connectivity option for Contoso is a multi-point connection with multiple peering locations around the globe to service the needs of their employees in each continent. Each continent includes redundant Azure ExpressRoute circuits within the continent and security must span all of these.

Contoso's existing infrastructure is reliable and can handle the extra work, as a result, Contoso is able to use the infrastructure for their Azure ExpressRoute and internet perimeter security. If this weren't the case, Contoso could choose to purchase more equipment to supplement their existing equipment or to handle a different type of connection.

High availability and failover with Azure ExpressRoute

We recommend provisioning at least two active circuits from each egress with ExpressRoute to your ExpressRoute provider. This is the most common place we see failures for customers and you can easily avoid it by provisioning a pair of active/active ExpressRoute circuits. We also recommend at least two active/active Internet circuits because many Office 365 services are only available over the Internet.

Inside the egress point of your network are many other devices and circuits that play a critical role in how people perceive availability. These portions of your connectivity scenarios are not covered by ExpressRoute or Office 365 SLAs, but they play a critical role in the end-to-end service availability as perceived by people in your organization.

Focus on the people using and operating Office 365, if a failure of any one component would affect peoples' experience using the service, look for ways to limit the total percentage of people affected. If a failover mode is operationally complex, consider the peoples' experience of a long time to recovery and look for operationally simple and automated failover modes.

Outside of your network, Office 365, ExpressRoute, and your ExpressRoute provider all have different levels of availability.

Service Availability

- Office 365 services are covered by well-defined [service level agreements](#), which include uptime and availability metrics for individual services. One reason Office 365 can maintain such high service availability levels is the ability for individual components to seamlessly fail over between the many Microsoft datacenters, using the global Microsoft network. This failover extends from the datacenter and network to the multiple Internet egress points, and enables failover seamlessly from the perspective of the people using the service.
- ExpressRoute [provides a 99.9% availability SLA](#) on individual dedicated circuits between the Microsoft Network Edge and the ExpressRoute provider or partner infrastructure. These service levels are applied at the ExpressRoute circuit level, which consists of [two independent interconnects](#) between the redundant Microsoft equipment and the network provider equipment in each peering location.

Provider Availability

- Microsoft's service level arrangements stop at your ExpressRoute provider or partner. This is also the first place you can make choices that will influence your availability level. You should closely evaluate the architecture, availability, and resiliency characteristics your ExpressRoute provider offers between your network perimeter and your providers connection at each Microsoft peering location. Pay close attention to both the logical and physical aspects of redundancy, peering equipment, carrier provided WAN circuits, and any extra value add services such as NAT services or managed firewalls.

Designing your availability plan

We strongly recommend that you plan and design high availability and resiliency into your end-to-end connectivity scenarios for Office 365. A design should include;

- No single points of failure, including both Internet and ExpressRoute circuits.

- Minimizing the number of people affected and duration of that impact for most anticipated failure modes.
- Optimizing for simple, repeatable, and automatic recovery process from most anticipated failure modes.
- Supporting the full demands of your network traffic and functionality through redundant paths, without substantial degradation.

Your connectivity scenarios should include a network topology that is optimized for multiple independent and active network paths to Office 365. This will yield a better end-to-end availability than a topology that is optimized only for redundancy at the individual device or equipment level.

TIP

If your users are distributed across multiple continents or geographic regions and each of those locations connects over redundant WAN circuits to a single on-premises location where a single ExpressRoute circuit is located, your users will experience less end-to-end service availability than a network topology design that includes independent ExpressRoute circuits that connect the different regions to the nearest peering location.

We recommend provisioning at least two ExpressRoute circuits with each circuit connecting to with a different geographic peering location. You should provision this active-active pair of circuits for every region where people will use ExpressRoute connectivity for Office 365 services. This allows each region to remain connected during a disaster that affects a major location such as a datacenter or peering location. Configuring them in as active/active allows end user traffic to be distributed across multiple network paths. This reduces the scope of people affected during device or network equipment outages.

We don't recommend using a single ExpressRoute circuit with the Internet as a backup.

Example 2: Failover and High Availability

Contoso's multi-geographic design has undergone a review of routing, bandwidth, security, and now must go through a high availability review. Contoso thinks about high availability as covering three categories; resiliency, reliability, and redundancy.

Resiliency allows Contoso to recover from failures quickly. Reliability allows Contoso to offer a consistent outcome within the system. Redundancy allows Contoso to a move between one or more mirrored instances of infrastructure.

Within each edge configuration, Contoso has redundant Firewalls, Proxies, and IDS. For North America, Contoso has one edge configuration in their Dallas datacenter and another edge configuration in their Virginia datacenter. The redundant equipment at each location offers resiliency to that location.

The network configuration at Contoso is built based on a few key principles:

- Within each geographic region, there are multiple Azure ExpressRoute circuits.
- Each circuit within a region can support all of the network traffic within that region.
- Routing will clearly prefer one or the other path depending on availability, location, and so on.
- Failover between Azure ExpressRoute circuits happens automatically without additional configuration or action required by Contoso.
- Failover between Internet circuits happens automatically without additional configuration or action required by Contoso.

In this configuration, with redundancy at the physical and virtual level, Contoso is able to offer local resiliency, regional resiliency, and global resiliency in a reliable way. Contoso elected this configuration after evaluating a single Azure ExpressRoute circuit per region as well as the possibility of failing over to the internet.

If Contoso was unable to have multiple Azure ExpressRoute circuits per region, routing traffic originating in North America to the Azure ExpressRoute circuit in Asia Pacific would add an unacceptable level of latency and the required DNS forwarder configuration adds complexity.

Using the internet as a backup configuration isn't recommended. This breaks Contoso's reliability principle, resulting in an inconsistent experience using the connection. Additionally, manual configuration would be required to fail over considering the BGP advertisements that have been configured, NAT configuration, DNS configuration, and the proxy configuration. This added failover complexity increases the time to recover and decreases their ability to diagnose and troubleshoot the steps involved.

Still have questions about how to plan for and implement traffic management or Azure ExpressRoute? Read the rest of our [network and performance guidance](#) or the [Azure ExpressRoute FAQ](#).

Working with Azure ExpressRoute providers

Choose the locations of your circuits based on your bandwidth, latency, security, and high availability planning. Once you know the optimal locations, you'd like to place circuits [review the current list of providers by region](#).

Work with your provider or providers to select the best connectivity options, point-to-point, multi-point, or hosted. Remember, you can mix and match the connectivity options so long as the bandwidth and other redundant components support your routing and high availability design.

Here's a short link you can use to come back: <https://aka.ms/planningexpressroute365>

Related Topics

[Assessing Office 365 network connectivity](#)

[Azure ExpressRoute for Office 365](#)

[Managing ExpressRoute for Office 365 connectivity](#)

[Routing with ExpressRoute for Office 365](#)

[Implementing ExpressRoute for Office 365](#)

[Using BGP communities in ExpressRoute for Office 365 scenarios](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Optimizing your network for Skype for Business Online](#)

[ExpressRoute and QoS in Skype for Business Online](#)

[Call flow using ExpressRoute](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 network and performance tuning](#)

[Office 365 endpoints FAQ](#)

Plan for network devices that connect to Office 365 services

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Some network hardware may have limitations on the number of concurrent sessions that are supported. For organizations having more than 2,000 users, we recommend that they monitor their network devices to ensure they're capable of handling the additional Office 365 service traffic. Simple Network Management Protocol (SNMP) monitoring software can help you do this.

This article is part of [Network planning and performance tuning for Office 365](#).

On-premises outgoing Internet proxy settings also affect connectivity to Office 365 services for your client applications. You must also configure your network proxy devices to allow connections for Microsoft cloud services URLs and applications. Every organization is different. To get an idea for how Microsoft manages this process and the amount of bandwidth we provision, [read the case study](#).

The following Skype for Business Help articles have more information about Skype for Business settings:

- [Troubleshooting Skype for Business Online sign-in errors for administrators](#)
- [You cannot connect to Skype for Business, or certain features don't work, because an on-premises firewall blocks the connection](#)

NOTE

While many of these settings are Skype for Business-specific, the general guidance on network configuration is useful for all Office 365 services.

Determining Network Capacity

Every network device that exists on a connection has its capacity limit. These devices include the client and server network adapters, routers, switches, and hubs that interconnect them. Adequate network capacity means that none of them are saturated. Monitoring network activity is essential to help ensure that the actual loads on all network devices are less than their maximum capacity. Network capacity affects proxy device performance.

In most situations, the Internet connection bandwidth sets the limit for the amount of traffic. Weak performance during peak traffic hours is probably caused by excessive use of the Internet link. This situation also applies to a branch office scenario, where branch office proxy server computers are connected to the proxy device at the branch's headquarters over a slow Wide Area Network (WAN) link.

To test network capacity, monitor the network activity on the proxy network interface. If it's more than 75 percent of the maximum bandwidth of any network interface, consider increasing the bandwidth of the network infrastructure that's inadequate. Or, consider using advanced features, such as HTTP compression.

WAN Accelerators

If your organization uses wide area network (WAN) acceleration proxy appliances, you may encounter issues when you access the Office 365 services. You may need to optimize your network device or devices to ensure that your users have a consistent experience when accessing Office 365. For example, Office 365 services

encrypt some Office 365 content and the TCP header. Your device may not be able to handle this kind of traffic.

Read our support statement about [Using WAN Optimization Controller or Traffic/Inspection devices with Office 365](#).

Hardware and Software Load-balancing Devices

Your organization needs to use a hardware load balancer (HLB) or a Network Load Balancing (NLB) solution to distribute requests to your Active Directory Federation Services (AD FS) servers and/or your Exchange hybrid servers. Load-balancing devices control the network traffic to the on-premises servers. These servers are crucial in helping to ensure the availability of single sign-on and Exchange hybrid deployment.

We provide a software-based NLB solution built into Windows Server. Office 365 supports this solution to achieve load balancing.

Firewalls and proxies

For more details on configuring firewalls and proxies to connect to Office 365, read [Managing Office 365 endpoints](#), [Assessing Office 365 network connectivity](#), and [Office 365 endpoints FAQ](#) to learn more about devices and circuit selection.

See also

[Setup guides for Office 365 services](#)

[Microsoft 365 Enterprise overview](#)

Network and migration planning for Office 365

10/28/2022 • 4 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

This article contains links to information about network planning and testing, and migration to Office 365.

Before you deploy for the first time or migrate to Office 365, you can use the information in these topics to estimate the bandwidth you need and then to test and verify that you have enough bandwidth to deploy or migrate to Office 365.

This article is part of [Network planning and performance tuning for Office 365](#).

For the steps to optimize your network for Microsoft 365 and other Microsoft cloud platforms and services, see the [Microsoft Cloud Networking for Enterprise Architects](#) poster.

Estimate network bandwidth requirements

Using Office 365 may increase the utilization of your organization's internet circuit. It's important to determine if the amount of bandwidth currently available is enough to handle the estimated increase once Office 365 is fully deployed while leaving at least 20% capacity to handle the busiest of days.

To estimate the bandwidth, use the following steps:

1. Assess the number of clients that will use each Internet egress. Let our multi-terabit network handle as much of the connection as possible.
2. Determine which Office 365 services and features will be available for clients to use. You will likely have groups of people with different services or usage profiles.
3. Measure the network use for a pilot group of clients. Ensure the pilot clients are representative of the different profiles of people in the organization as well as the different geographic locations. You can cross-check your results against our old calculators for [Exchange](#) and [Microsoft Teams](#) or the [case study](#) we performed on our own network.
4. Use the measurements from the pilot group to extrapolate the entire organization's needs and re-test to validate the estimations before making any changes to your network.

Test your existing network

Network tools. Test and validate your Internet bandwidth to determine download, upload, and latency constraints. These tools will help you determine the capabilities of your network for migration as well as after you're fully deployed.

- [Microsoft Remote Connectivity Analyzer](#): Tests connectivity in your Exchange Online environment.
- Use the [Microsoft Support and Recovery Assistant for Office 365](#) to fix Outlook and Office 365 problems.
- [Microsoft 365 network connectivity test tool](#): Tests Microsoft 365 network connectivity.

Best practices for network planning and improving migration performance for Office 365

Dig a little deeper into these best practices for more information about improving your Office 365 experience.

1. Want to get started helping your users right away? See [Best practices for using Office 365 on a slow network](#) for tips on using Office 365, including SharePoint Online, Exchange Online, and Lync Online, when your network just isn't cooperating. This article links out to loads of content on TechNet and Support.office.com for optimizing your Office 365 experience and includes information on easy ways to customize your web pages and how to set your Internet Explorer settings for the best Office 365 experience.
2. Read [Office 365 Network Connectivity Principles](#) to understand the connectivity principles for securely managing Office 365 traffic and getting the best possible performance. This article will help you understand the most recent guidance for securely optimizing Office 365 network connectivity.
3. Improve mail migration performance by carefully managing the schedule for Windows Updates. You can update your client computers in batches and ensure that all client computers are updated before migrating to Office 365 to regulate the use of network bandwidth. For more information, see [Manually update and configure desktops for Office 365 for the latest updates](#).
4. Office 365 network traffic performs best when it's treated as a trusted Internet service and allowed to bypass much of the traditional filtering and scanning that some organizations place on network traffic to untrusted Internet services. This typically includes removing outbound processing such as proxy user authentication and packet inspection, as well as ensuring local egress to the Internet with the proper Network Address Translation (NAT) and enough bandwidth capacity to handle the increased network requests. Refer to [Managing Office 365 endpoints](#) for additional guidance on configuring your network to handle Office 365 as a trusted Internet service on your network.
5. Ensure [Managing Office 365 endpoints](#). The additional traffic going to Office 365 results in an increase of outbound proxy connections as well as an increase in secure traffic over TLS/SSL.
6. If your outbound proxies require user authentication you may experience slow connectivity or a loss of functionality. Bypassing the authentication requirement for the Office 365 domains can reduce this overhead.
7. If you have a large number of shared calendars and mailboxes, you may see an increase in the number of connections from Outlook to Exchange. For instance, the Outlook client may open up to two additional connections for each shared calendar in use. In this situation, ensure that the egress proxy can handle the connections, or bypass the proxy for connections to Office 365 for Outlook.
8. Determine the maximum number of supported devices for a public IP address and how to load balance across multiple IP addresses. For more information, see [NAT support with Office 365](#).
9. If you're inspecting outbound connections from computers on your network, bypassing this filtering to the Office 365 domains will improve connectivity and performance. Additionally, bypassing outbound inspection often removes the need for a single Internet egress and enables local Internet egress for Office 365 destined network requests.
10. Some customers find internal network settings may affect performance. Settings such as maximum transmission unit (MTU) size, network auto-negotiation or auto-detection, and sub-optimal routes to the Internet are common places to look.

Network planning reference for Office 365

These topics contain detailed Office 365 network reference information.

- [Managing Office 365 endpoints](#)
- [Content delivery networks](#)

- [External Domain Name System records for Office 365](#)
- [IPv6 support in Office 365 services](#)
- [Office 365 Network Connectivity Principles](#)
- [Plan for network devices that connect to Office 365 services](#)
- [Setup guides for Office 365 services](#)

See also

[Microsoft 365 Enterprise overview](#)

Add a domain to Microsoft 365

10/28/2022 • 5 minutes to read • [Edit Online](#)

[Check the Domains FAQ](#) if you don't find what you're looking for.

Check out [Microsoft 365 small business help](#) on YouTube.

Before you begin

To add, modify, or remove domains, you **must** be a **Domain Name Administrator** or **Global Administrator** of a [business or enterprise plan](#). These changes affect the whole tenant; *Customized administrators* or *regular users* won't be able to make these changes.

TIP

If you need help with the steps in this topic, consider [working with a Microsoft small business specialist](#). With Business Assist, you and your employees get around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use.

Watch: Add a domain

Check out this video and others on our [YouTube channel](#).

Your company might need multiple domain names for different purposes. For example, you might want to add a different spelling of your company name because customers are already using it and their communications have failed to reach you.

1. In the Microsoft 365 admin center, choose **Setup**.
2. Under **Get your custom domain set up**, select **View** > **Manage** > **Add domain**.
3. Enter the new domain name that you want to add, and then select **Next**.
4. Sign in to your domain registrar, and then select **Next**.
5. Choose the services for your new domain.
6. Select **Next** > **Authorize** > **Next**, and then **Finish**. Your new domain has been added.

Add a domain

Follow these steps to add, set up, or continue setting up a domain.

1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to the **Settings** > **Domains** page.
3. Select **Add domain**.
4. Enter the name of the domain you want to add, then select **Next**.
5. Choose how you want to verify that you own the domain.
 - a. If your domain registrar uses [Domain Connect](#), Microsoft [will set up your records automatically](#) by

having you sign in to your registrar and confirm the connection to Microsoft 365. You'll be returned to the admin center and Microsoft will then automatically verify your domain.

b. You can use a TXT record to verify your domain. Select this and select **Next** to see instructions for how to add this DNS record to your registrar's website. This can take up to 30 minutes to verify after you've added the record.

c. You can add a text file to your domain's website. Select and download the .txt file from the setup wizard, then upload the file to your website's top level folder. The path to the file should look similar to: `http://mydomain.com/ms39978200.txt`. We'll confirm you own the domain by finding the file on your website.

6. Choose how you want to make the DNS changes required for Microsoft to use your domain.

a. Choose **Add the DNS records for me** if your registrar supports [Domain Connect](#), and Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365.

b. Choose **I'll add the DNS records myself** if you want to attach only specific Microsoft 365 services to your domain or if you want to skip this for now and do this later. **Choose this option if you know exactly what you're doing.**

7. If you chose to *add DNS records yourself*, select **Next** and you'll see a page with all the records that you need to add to your registrar's website to set up your domain.

If the portal doesn't recognize your registrar, you can [follow these general instructions](#).

If you don't know the DNS hosting provider or domain registrar for your domain, see [Find your domain registrar or DNS hosting provider](#).

If you want to wait for later, either unselect all the services and click **Continue**, or in the previous domain connection step choose **More Options** and select **Skip this for now**.

8. Select **Finish** - you're done!

Add or edit custom DNS records

Follow the steps below to add a custom record for a website or 3rd party service.

1. Sign in to the Microsoft admin center at <https://admin.microsoft.com>.
2. Go to the **Settings > Domains** page.
3. On the **Domains** page, select a domain.
4. Under **DNS settings**, select **Custom Records**; then select **New custom record**.
5. Select the type of DNS record you want to add and type the information for the new record.
6. Select **Save**.

Registrars with Domain Connect

[Domain Connect](#) enabled registrars let you add your domain to Microsoft 365 in a three-step process that takes minutes.

In the wizard, we'll just confirm that you own the domain, and then automatically set up your domain's records, so email comes to Microsoft 365 and other Microsoft 365 services, like Teams, work with your domain.

NOTE

Make sure you disable any popup blockers in your browser before you start the setup wizard.

Domain Connect registrars integrating with Microsoft 365

- [1&1 IONOS](#)
- [EuroDNS](#)
- [Cloudflare](#)
- [GoDaddy](#)
- [WordPress.com](#)
- [Plesk](#)
- [MediaTemple](#)
- SecureServer or WildWestDomains (GoDaddy resellers using SecureServer DNS hosting)
 - Examples:
 - [DomainsPricedRight](#)
 - [DomainRightNow](#)

What happens to my email and website?

After you finish setup, the MX record for your domain is updated to point to Microsoft 365 and all email for your domain will start coming to Microsoft 365. Make sure you've added users and set up mailboxes in Microsoft 365 for everyone who gets email on your domain!

If you have a website that you use with your business, it will keep working where it is. The Domain Connect setup steps don't affect your website.

Add an onmicrosoft.com domain

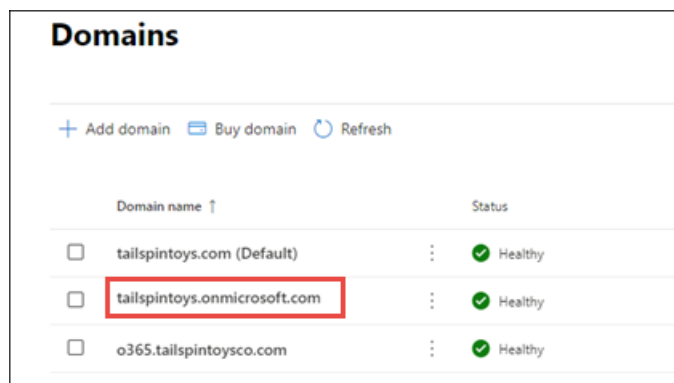
Each Microsoft 365 organization can have up to five onmicrosoft.com domains.

NOTE

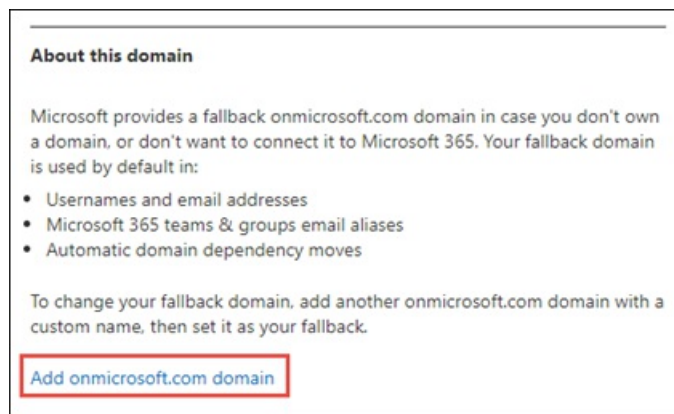
You must be a Global admin or a Domain Name admin to add a domain. Creating an additional .onmicrosoft domain and using it as your default will not do a rename for SharePoint Online. To make changes to your .onmicrosoft SharePoint domain you would need to use the [SharePoint domain rename preview](#) (currently available to any tenant with less than 10,000 sites). If you're using Microsoft 365 mail services, removal of your initial .onmicrosoft domain is not supported.

To add an onmicrosoft.com domain:

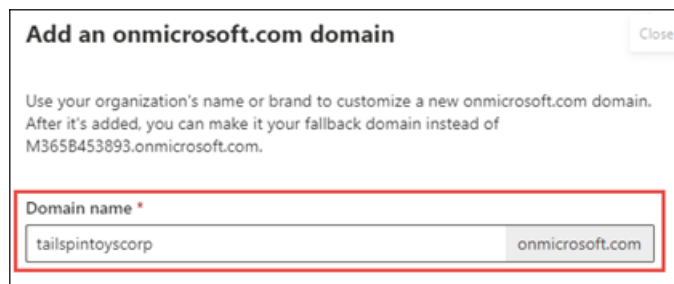
1. In the Microsoft 365 admin center, select **Settings**, and then select **Domains**.
2. Select an existing *.onmicrosoft.com* domain.



3. On the **Overview** tab, select **Add onmicrosoft.com domain**.



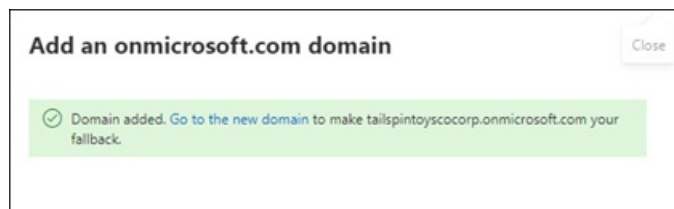
4. On the **Add onmicrosoft.com domain** page, in the **Domain name** box, enter the name for your new onmicrosoft.com domain.



NOTE

Make sure to verify the spelling and accuracy of the domain name you entered. You are limited to five onmicrosoft.com domains, and currently they cannot be deleted once they are created.

5. Select **Add domain**. When successfully added, you will see a message stating this.



You can set any domain you own as your default domain.

For more details on how to add an onmicrosoft.com domain, see [Add or replace your onmicrosoft.com domain](#).

Related content

[Domains FAQ](#) (article)

[What is a domain?](#) (article)

[Buy a domain name in Microsoft 365](#) (article)

[Add DNS records to connect your domain](#) (article)

[Change nameservers to set up Microsoft 365 with any domain registrar](#) (article)

Office 365 IP Address and URL web service

10/28/2022 • 22 minutes to read • [Edit Online](#)

The Office 365 IP Address and URL web service helps you better identify and differentiate Office 365 network traffic, making it easier for you to evaluate, configure, and stay up to date with changes. This REST-based web service replaces the previous XML downloadable files, which were phased out on October 2, 2018.

As a customer or a network perimeter device vendor, you can build against the web service for Office 365 IP address and FQDN entries. You can access the data directly in a web browser using these URLs:

- For the latest version of the Office 365 URLs and IP address ranges, use <https://endpoints.office.com/version>.
- For the data on the Office 365 URLs and IP address ranges page for firewalls and proxy servers, use <https://endpoints.office.com/endpoints/worldwide>.
- To get all the latest changes since July 2018 when the web service was first available, use <https://endpoints.office.com/changes/worldwide/0000000000>.

As a customer, you can use this web service to:

- Update your PowerShell scripts to obtain Office 365 endpoint data and modify any formatting for your networking devices.
- Use this information to update PAC files deployed to client computers.

As a network perimeter device vendor, you can use this web service to:

- Create and test device software to download the list for automated configuration.
- Check for the current version.
- Get the current changes.

NOTE

If you are using Azure ExpressRoute to connect to Office 365, please review [Azure ExpressRoute for Office 365](#) to familiarize yourself with the Office 365 services supported over Azure ExpressRoute. Also review the article [Office 365 URLs and IP address ranges](#) to understand which network requests for Office 365 applications require Internet connectivity. This will help to better configure your perimeter security devices.

For more information, see:

- [Announcement blog post in the Office 365 Tech Community Forum](#)
- [Office 365 Tech Community Forum for questions about use of the web services](#)

Common parameters

These parameters are common across all the web service methods:

- **format= <JSON | CSV>** —By default, the returned data format is JSON. Use this optional parameter to return the data in comma-separated values (CSV) format.
- **ClientRequestId= <guid>** —A required GUID that you generate for client association. Generate a unique GUID for each machine that calls the web service (the scripts included on this page generate a GUID for you). Do not use the GUIDs shown in the following examples because they might be blocked by the web service in the future. GUID format is `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`, where x represents a hexadecimal number.

To generate a GUID, you can use the [New-Guid](#) PowerShell command, or use an online service such as [Online GUID Generator](#).

Version web method

Microsoft updates the Office 365 IP address and FQDN entries at the beginning of each month. Out-of-band updates are sometimes published due to support incidents, security updates or other operational requirements.

The data for each published instance is assigned a version number, and the version web method enables you to check for the latest version of each Office 365 service instance. We recommend that you check the version not more than once an hour.

Parameters for the version web method are:

- **AllVersions= <true | false>** —By default, the version returned is the latest. Include this optional parameter to request all published versions since the web service was first released.
- **Format= <JSON | CSV | RSS>** —In addition to the JSON and CSV formats, the version web method also supports RSS. You can use this optional parameter along with the *AllVersions=true* parameter to request an RSS feed that can be used with Outlook or other RSS readers.
- **Instance= <Worldwide | China | USGovDoD | USGovGCCHigh>** —This optional parameter specifies the instance to return the version for. If omitted, all instances are returned. Valid instances are: Worldwide, China, USGovDoD, USGovGCCHigh.

The version web method is not rate limited and does not ever return 429 HTTP Response Codes. The response to the version web method does include a cache-control header recommending caching of the data for 1 hour. The result from the version web method can be a single record or an array of records. The elements of each record are:

- **instance**—The short name of the Office 365 service instance.
- **latest**—The latest version for endpoints of the specified instance.
- **versions**—A list of all previous versions for the specified instance. This element is only included if the *AllVersions* parameter is true.

Version web method examples

Example 1 request URI: <https://endpoints.office.com/version?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This URI returns the latest version of each Office 365 service instance. Example result:

```
[
  {
    "instance": "Worldwide",
    "latest": "2018063000"
  },
  {
    "instance": "USGovDoD",
    "latest": "2018063000"
  },
  {
    "instance": "USGovGCCHigh",
    "latest": "2018063000"
  },
  {
    "instance": "China",
    "latest": "2018063000"
  }
]
```

IMPORTANT

The GUID for the ClientRequestId parameter in these URIs are only an example. To try the web service URIs out, generate your own GUID. The GUIDs shown in these examples may be blocked by the web service in the future.

Example 2 request URI: <https://endpoints.office.com/version/Worldwide?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This URI returns the latest version of the specified Office 365 service instance. Example result:

```
{
  "instance": "Worldwide",
  "latest": "2018063000"
}
```

Example 3 request URI: <https://endpoints.office.com/version/Worldwide?Format=CSV&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This URI shows output in CSV format. Example result:

```
instance,latest
Worldwide,2018063000
```

Example 4 request URI: <https://endpoints.office.com/version/Worldwide?AllVersions=true&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This URI shows all prior versions that have been published for the Office 365 worldwide service instance.
Example result:

```
{
  "instance": "Worldwide",
  "latest": "2018063000",
  "versions": [
    "2018063000",
    "2018062000"
  ]
}
```

Example 5 RSS Feed URI: <https://endpoints.office.com/version/worldwide?clientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7&allVersions=true&format=RSS>

This URI shows an RSS feed of the published versions that include links to the list of changes for each version.
Example result:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<rss version="2.0" xmlns:atom="https://www.w3.org/2005/Atom">
<channel>
<link>https://aka.ms/o365ip</link>
<description/>
<language>en-us</language>
<lastBuildDate>Thu, 02 Aug 2018 00:00:00 Z</lastBuildDate>
<item>
<guid isPermaLink="false">2018080200</guid>
<link>https://endpoints.office.com/changes/Worldwide/2018080200?singleVersion&clientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7</link> <description>Version 2018080200 includes 2 changes. IPs: 2 added and 0 removed.</description>
<pubDate>Thu, 02 Aug 2018 00:00:00 Z</pubDate>
</item>
```

Endpoints web method

The endpoints web method returns all records for IP address ranges and URLs that make up the Office 365 service. The latest data from the endpoints web method should always be used for network device configuration. Microsoft provides advance notice 30 days prior to publishing new additions to give you time to update access control lists and proxy server bypass lists. We recommend that you only call the endpoints web method again when the version web method indicates that a new version of the data is available.

Parameters for the endpoints web method are:

- **ServiceAreas=** <Common | Exchange | SharePoint | Skype> —A comma-separated list of service areas. Valid items are *Common*, *Exchange*, *SharePoint*, and *Skype*. Because *Common* service area items are a prerequisite for all other service areas, the web service always includes them. If you do not include this parameter, all service areas are returned.
- **TenantName=** <tenant_name> —Your Office 365 tenant name. The web service takes your provided name and inserts it in parts of URLs that include the tenant name. If you don't provide a tenant name, those parts of URLs have the wildcard character (*).
- **NoIPv6=** <true | false> —Set the value to *true* to exclude IPv6 addresses from the output if you don't use IPv6 in your network.
- **Instance=** <Worldwide | China | USGovDoD | USGovGCCHigh> —This required parameter specifies the instance from which to return the endpoints. Valid instances are: *Worldwide*, *China*, *USGovDoD*, and *USGovGCCHigh*.

If you call the endpoints web method too many times from the same client IP address, you might receive HTTP response code *429 (Too Many Requests)*. If you get this response code, wait 1 hour before repeating your request, or generate a new GUID for the request. As a general best practice, only call the endpoints web method when the version web method indicates that a new version is available.

The result from the endpoints web method is an array of records in which each record represents a specific endpoint set. The elements for each record are:

- **id**—The immutable ID number of the endpoint set.
- **serviceArea**—The service area that this is part of: *Common*, *Exchange*, *SharePoint*, or *Skype*.
- **urls**—URLs for the endpoint set. A JSON array of DNS records. Omitted if blank.
- **tcpPorts**—TCP ports for the endpoint set. All ports elements are formatted as a comma-separated list of ports or port ranges separated by a dash character (-). Ports apply to all IP addresses and all URLs in the endpoint set for a given category. Omitted if blank.
- **udpPorts**—UDP ports for the IP address ranges in this endpoint set. Omitted if blank.
- **ips** —The IP address ranges associated with this endpoint set as associated with the listed TCP or UDP ports. A JSON array of IP address ranges. Omitted if blank.

- **category**—The connectivity category for the endpoint set. Valid values are *Optimize*, *Allow*, and *Default*. If you search the endpoints web method output for the category of a specific IP address or URL, it is possible that your query will return multiple categories. In such a case, follow the recommendation for the highest priority category. For example, if the endpoint appears in both *Optimize* and *Allow*, you should follow the requirements for *Optimize*. Required.
- **expressRoute** — *True* if this endpoint set is routed over ExpressRoute, *False* if not.
- **required** — *True* if this endpoint set is required to have connectivity for Office 365 to be supported. *False* if this endpoint set is optional.
- **notes**—For optional endpoints, this text describes Office 365 functionality that would be unavailable if IP addresses or URLs in this endpoint set cannot be accessed at the network layer. Omitted if blank.

Endpoints web method examples

Example 1 request URI: <https://endpoints.office.com/endpoints/Worldwide?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This URI obtains all endpoints for the Office 365 worldwide instance for all workloads. Example result that shows an excerpt of the output:

```
[
  {
    "id": 1,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls":
    [
      ".*.protection.outlook.com"
    ],
    "ips":
    [
      "2a01:111:f403::/48", "23.103.132.0/22", "23.103.136.0/21", "23.103.198.0/23", "23.103.212.0/22",
      "40.92.0.0/14", "40.107.0.0/17", "40.107.128.0/18", "52.100.0.0/14", "213.199.154.0/24",
      "213.199.180.128/26", "94.245.120.64/26", "207.46.163.0/24", "65.55.88.0/24", "216.32.180.0/23",
      "23.103.144.0/20", "65.55.169.0/24", "207.46.100.0/24", "2a01:111:f400:7c00::/54", "157.56.110.0/23",
      "23.103.200.0/22", "104.47.0.0/17", "2a01:111:f400:fc00::/54", "157.55.234.0/24", "157.56.112.0/24",
      "52.238.78.88/32"
    ],
    "tcpPorts": "443",
    "expressRoute": true,
    "category": "Allow"
  },
  {
    "id": 2,
    "serviceArea": "Exchange",
    "serviceAreaDisplayName": "Exchange Online",
    "urls":
    [
      ".*.mail.protection.outlook.com"
    ],
    "ips":
    [

```

The full output of the request in this example would contain other endpoint sets.

Example 2 request URI: <https://endpoints.office.com/endpoints/Worldwide?ServiceAreas=Exchange&ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This example obtains endpoints for the Office 365 Worldwide instance for Exchange Online and dependencies only.

The output, for example, 2 is similar to example 1 except that the results would not include endpoints for SharePoint Online or Skype for Business Online.

Changes web method

The changes web method returns the most recent updates that have been published, typically the previous month's changes to IP address ranges and URLs.

The most critical changes to endpoints data are new URLs and IP addresses. Failure to add an IP address to a firewall access control list or a URL to a proxy server bypass list can cause an outage for Office 365 users behind that network device. Notwithstanding operational requirements, new endpoints are published to the web service 30 days in advance of the date the endpoints are provisioned for use to give you time to update access control lists and proxy server bypass lists.

The required parameter for the changes web method is:

- **Version= <YYYYMMDDNN>** —Required URL route parameter. This value is the version that you have currently implemented. The web service will return the changes since that version. The format is *YYYYMMDDNN*, where *NN* is a natural number incremented if there are multiple versions required to be published on a single day, with *00* representing the first update for a given day. The web service requires the *version* parameter to contain exactly 10 digits.

The changes web method is rate limited in the same way as the endpoints web method. If you receive a 429 HTTP response code, wait 1 hour before repeating your request or generate a new GUID for the request.

The result from the changes web method is an array of records in which each record represents a change in a specific version of the endpoints. The elements for each record are:

- **id**—The immutable ID of the change record.
- **endpointSetId**—The ID of the endpoint set record that is changed.
- **disposition**—Describes what the change did to the endpoint set record. Values are *change*, *add*, or *remove*.
- **impact**—Not all changes will be equally important to every environment. This element describes the expected impact to an enterprise network perimeter environment as a result of this change. This element is included only in change records of version **2018112800** and later. Options for the impact are: — **AddedIp** – An IP address was added to Office 365 and will be live on the service soon. This represents a change you need to take on a firewall or other layer 3 network perimeter device. If you don't add this before we start using it, you may experience an outage. — **AddedUrl** – A URL was added to Office 365 and will be live on the service soon. This represents a change you need to take on a proxy server or URL parsing network perimeter device. If you don't add this URL before we start using it, you may experience an outage. — **AddedIpAndUrl** —Both an IP address and a URL were added. This represents a change you need to take on either a firewall layer 3 device or a proxy server or URL parsing device. If you don't add this IP/URL pair before we start using it, you may experience an outage. — **RemovedIpOrUrl** – At least one IP address or URL was removed from Office 365. Remove the network endpoints from your perimeter devices, but there's no deadline for you to do this. — **ChangedIsExpressRoute** – The ExpressRoute support attribute was changed. If you use ExpressRoute, you might need to take action depending on your configuration. — **MovedIpOrUrl** – We moved an IP address or Url between this endpoint set and another one. Generally no action is required. — **RemovedDuplicateIpOrUrl** – We removed a duplicate IP address or Url but it's still published for Office 365. Generally no action is required. — **OtherNonPriorityChanges** – We changed something less critical than all of the other options, such as the contents of a note field.
- **version**—The version of the published endpoint set in which the change was introduced. Version numbers are of the format *YYYYMMDDNN*, where *NN* is a natural number incremented if there are multiple versions required to be published on a single day.
- **previous**—A substructure detailing previous values of changed elements on the endpoint set. This will not be included for newly added endpoint sets. Includes *ExpressRoute*, *serviceArea*, *category*, *required*, *tcpPorts*, *udpPorts*, and *notes*.
- **current**—A substructure detailing updated values of changes elements on the endpoint set. Includes *ExpressRoute*, *serviceArea*, *category*, *required*, *tcpPorts*, *udpPorts*, and *notes*.

- add —A substructure detailing items to be added to endpoint set collections. Omitted if there are no additions. — effectiveDate—Defines the data when the additions will be live in the service. — ips—Items to be added to the *ips* array. — urls- Items to be added to the *urls* array.
- remove—A substructure detailing items to be removed from the endpoint set. Omitted if there are no removals. — ips—Items to be removed from the *ips* array. — urls- Items to be removed from the *urls* array.

Changes web method examples

Example 1 request URI: <https://endpoints.office.com/changes/worldwide/0000000000?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This requests all previous changes to the Office 365 worldwide service instance. Example result:

```
[
  {
    "id": 424,
    "endpointSetId": 32,
    "disposition": "Change",
    "version": "2018062700",
    "remove":
    {
      "urls":
      [
        "*.api.skype.com", "skypegraph.skype.com"
      ]
    }
  },
  {
    "id": 426,
    "endpointSetId": 31,
    "disposition": "Change",
    "version": "2018062700",
    "add":
    {
      "effectiveDate": "20180609",
      "ips":
      [
        "51.140.203.190/32"
      ]
    },
    "remove":
    {
      "ips":
      [
```

Example 2 request URI: <https://endpoints.office.com/changes/worldwide/2018062700?ClientRequestId=b10c5ed1-bad1-445f-b386-b919946339a7>

This requests changes since the specified version to the Office 365 Worldwide instance. In this case, the version specified is the latest. Example result:

```
[
  {
    "id":3,
    "endpointSetId":33,
    "changeDescription":"Removing old IP prefixes",
    "disposition":"Change",
    "version":"2018031301",
    "remove":{
      "ips":["65.55.127.0/24","66.119.157.192/26","66.119.158.0/25",
        "111.221.76.128/25","111.221.77.0/26","207.46.5.0/24"]
    }
  },
  {
    "id":4,
    "endpointSetId":45,
    "changeDescription":"Removing old IP prefixes",
    "disposition":"Change",
    "version":"2018031301",
    "remove":{
      "ips":["13.78.93.8/32","40.113.87.220/32","40.114.149.220/32",
        "40.117.100.83/32","40.118.214.164/32","104.208.31.113/32"]
    }
  }
]
```

Example PowerShell script

You can run this PowerShell script to see if there are actions you need to take for updated data. You can run this script as a scheduled task to check for a version update. To avoid excessive load on the web service, try not to run the script more than once an hour.

The script does the following:

- Checks the version number of the current Office 365 Worldwide instance endpoints by calling the web service REST API.
- Checks for a current version file at *\$Env:TEMP\O365_endpoints_latestversion.txt*. The path of the global variable *\$Env:TEMP* is usually *C:\Users\<username>\AppData\Local\Temp*.
- If this is the first time the script has been run, the script returns the current version and all current IP addresses and URLs, writes the endpoints version to the file *\$Env:TEMP\O365_endpoints_latestversion.txt* and the endpoints data output to the file *\$Env:TEMP\O365_endpoints_data.txt*. You can modify the path and/or name of the output file by editing these lines:

```
$versionpath = $Env:TEMP + "\O365_endpoints_latestversion.txt"
$datapath = $Env:TEMP + "\O365_endpoints_data.txt"
```

- On each subsequent execution of the script, if the latest web service version is identical to the version in the *O365_endpoints_latestversion.txt* file, the script exits without making any changes.
- When the latest web service version is newer than the version in the *O365_endpoints_latestversion.txt* file, the script returns the endpoints and filters for the **Allow** and **Optimize** category endpoints, updates the version in the *O365_endpoints_latestversion.txt* file, and writes the updated data to the *O365_endpoints_data.txt* file.

The script generates a unique *ClientRequestId* for the computer it is executed on, and reuses this ID across multiple calls. This ID is stored in the *O365_endpoints_latestversion.txt* file.

To run the PowerShell script

1. Copy the script and save it to your local hard drive or script location as *Get-0365WebServiceUpdates.ps1*.
2. Execute the script in your preferred script editor such as the PowerShell ISE or VS Code, or from a PowerShell console using the following command:

```
powershell.exe -file <path>\Get-0365WebServiceUpdates.ps1
```

There are no parameters to pass to the script.

```
<# Get-0365WebServiceUpdates.ps1
From https://aka.ms/ipurlws
v1.1 8/6/2019

DESCRIPTION
This script calls the REST API of the Office 365 IP and URL Web Service (Worldwide instance)
and checks to see if there has been a new update since the version stored in an existing
$Env:TEMP\0365_endpoints_latestversion.txt file in your user directory's temp folder
(usually C:\Users\<username>\AppData\Local\Temp).
If the file doesn't exist, or the latest version is newer than the current version in the
file, the script returns IPs and/or URLs that have been changed, added or removed in the latest
update and writes the new version and data to the output file $Env:TEMP\0365_endpoints_data.txt.

USAGE
Run as a scheduled task every 60 minutes.

PARAMETERS
n/a

PREREQUISITES
PS script execution policy: Bypass
PowerShell 3.0 or later
Does not require elevation
#>

#Requires -Version 3.0

# web service root URL
$ws = "https://endpoints.office.com"
# path where output files will be stored
$versionpath = $Env:TEMP + "\0365_endpoints_latestversion.txt"
$datapath = $Env:TEMP + "\0365_endpoints_data.txt"

# fetch client ID and version if version file exists; otherwise create new file and client ID
if (Test-Path $versionpath) {
    $content = Get-Content $versionpath
    $clientRequestId = $content[0]
    $lastVersion = $content[1]
    Write-Output ("Version file exists! Current version: " + $lastVersion)
}
else {
    Write-Output ("First run! Creating version file at " + $versionpath + ".")
    $clientRequestId = [GUID]::NewGuid().Guid
    $lastVersion = "0000000000"
    @($clientRequestId, $lastVersion) | Out-File $versionpath
}

# call version method to check the latest version, and pull new data if version number is different
$version = Invoke-RestMethod -Uri ($ws + "/version/Worldwide?clientRequestId=" + $clientRequestId)
if ($version.latest -gt $lastVersion) {
    Write-Host "New version of Office 365 worldwide commercial service instance endpoints detected"
    # write the new version number to the version file
    @($clientRequestId, $version.latest) | Out-File $versionpath
    # invoke endpoints method to get the new data
    $endpointSets = Invoke-RestMethod -Uri ($ws + "/endpoints/Worldwide?clientRequestId=" +
```

```

$clientRequestId)
    # filter results for Allow and Optimize endpoints, and transform these into custom objects with port and
category
    # URL results
    $flatUrls = $endpointSets | ForEach-Object {
        $endpointSet = $_
        $urls = $(if ($endpointSet.urls.Count -gt 0) { $endpointSet.urls } else { @() })
        $urlCustomObjects = @()
        if ($endpointSet.category -in ("Allow", "Optimize")) {
            $urlCustomObjects = $urls | ForEach-Object {
                [PSCustomObject]@{
                    category = $endpointSet.category;
                    url      = $_;
                    tcpPorts = $endpointSet.tcpPorts;
                    udpPorts = $endpointSet.udpPorts;
                }
            }
        }
        $urlCustomObjects
    }

    # IPv4 results
    $flatIp4s = $endpointSets | ForEach-Object {
        $endpointSet = $_
        $ips = $(if ($endpointSet.ips.Count -gt 0) { $endpointSet.ips } else { @() })
        # IPv4 strings contain dots
        $ip4s = $ips | Where-Object { $_ -like '*.*' }
        $ip4CustomObjects = @()
        if ($endpointSet.category -in ("Allow", "Optimize")) {
            $ip4CustomObjects = $ip4s | ForEach-Object {
                [PSCustomObject]@{
                    category = $endpointSet.category;
                    ip       = $_;
                    tcpPorts = $endpointSet.tcpPorts;
                    udpPorts = $endpointSet.udpPorts;
                }
            }
        }
        $ip4CustomObjects
    }

    # IPv6 results
    $flatIp6s = $endpointSets | ForEach-Object {
        $endpointSet = $_
        $ips = $(if ($endpointSet.ips.Count -gt 0) { $endpointSet.ips } else { @() })
        # IPv6 strings contain colons
        $ip6s = $ips | Where-Object { $_ -like '*:*' }
        $ip6CustomObjects = @()
        if ($endpointSet.category -in ("Optimize")) {
            $ip6CustomObjects = $ip6s | ForEach-Object {
                [PSCustomObject]@{
                    category = $endpointSet.category;
                    ip       = $_;
                    tcpPorts = $endpointSet.tcpPorts;
                    udpPorts = $endpointSet.udpPorts;
                }
            }
        }
        $ip6CustomObjects
    }
}

# write output to screen
Write-Output ("Client Request ID: " + $clientRequestId)
Write-Output ("Last Version: " + $lastVersion)
Write-Output ("New Version: " + $version.latest)
Write-Output ""
Write-Output "IPv4 Firewall IP Address Ranges"
($flatIp4s.ip | Sort-Object -Unique) -join "," | Out-String
Write-Output "IPv6 Firewall IP Address Ranges"
($flatIp6s.ip | Sort-Object -Unique) -join "," | Out-String
Write-Output "URLs for Proxy Server"

```

```

($flatUrls.url | Sort-Object -Unique) -join "," | Out-String
Write-Output ("IP and URL data written to " + $datapath)

# write output to data file
Write-Output "Office 365 IP and UL Web Service data" | Out-File $datapath
Write-Output "Worldwide instance" | Out-File $datapath -Append
Write-Output "" | Out-File $datapath -Append
Write-Output ("Version: " + $version.latest) | Out-File $datapath -Append
Write-Output "" | Out-File $datapath -Append
Write-Output "IPv4 Firewall IP Address Ranges" | Out-File $datapath -Append
($flatIp4s.ip | Sort-Object -Unique) -join "," | Out-File $datapath -Append
Write-Output "" | Out-File $datapath -Append
Write-Output "IPv6 Firewall IP Address Ranges" | Out-File $datapath -Append
($flatIp6s.ip | Sort-Object -Unique) -join "," | Out-File $datapath -Append
Write-Output "" | Out-File $datapath -Append
Write-Output "URLs for Proxy Server" | Out-File $datapath -Append
($flatUrls.url | Sort-Object -Unique) -join "," | Out-File $datapath -Append
}
else {
    Write-Host "Office 365 worldwide commercial service instance endpoints are up-to-date."
}

```

Example Python Script

Here is a Python script, tested with Python 3.6.3 on Windows 10, that you can run to see if there are actions you need to take for updated data. This script checks the version number for the Office 365 Worldwide instance endpoints. When there is a change, it downloads the endpoints and filters for the *Allow* and *Optimize* category endpoints. It also uses a unique ClientRequestId across multiple calls and saves the latest version found in a temporary file. Call this script once an hour to check for a version update.

```

import json
import tempfile
from pathlib import Path
import urllib.request
import uuid
# helper to call the webservice and parse the response
def webApiGet(methodName, instanceName, clientRequestId):
    ws = "https://endpoints.office.com"
    requestPath = ws + '/' + methodName + '/' + instanceName + '?clientRequestId=' + clientRequestId
    request = urllib.request.Request(requestPath)
    with urllib.request.urlopen(request) as response:
        return json.loads(response.read().decode())
# path where client ID and latest version number will be stored
datapath = Path(tempfile.gettempdir() + '/endpoints_clientid_latestversion.txt')
# fetch client ID and version if data exists; otherwise create new file
if datapath.exists():
    with open(datapath, 'r') as fin:
        clientRequestId = fin.readline().strip()
        latestVersion = fin.readline().strip()
else:
    clientRequestId = str(uuid.uuid4())
    latestVersion = '0000000000'
    with open(datapath, 'w') as fout:
        fout.write(clientRequestId + '\n' + latestVersion)
# call version method to check the latest version, and pull new data if version number is different
version = webApiGet('version', 'Worldwide', clientRequestId)
if version['latest'] > latestVersion:
    print('New version of Office 365 worldwide commercial service instance endpoints detected')
    # write the new version number to the data file
    with open(datapath, 'w') as fout:
        fout.write(clientRequestId + '\n' + version['latest'])
    # invoke endpoints method to get the new data
    endpointSets = webApiGet('endpoints', 'Worldwide', clientRequestId)
    # filter results for Allow and Optimize endpoints, and transform these into tuples with port and
    category
    flatUrls = []
    for endpointSet in endpointSets:
        if endpointSet['category'] in ('Optimize', 'Allow'):
            category = endpointSet['category']
            urls = endpointSet['urls'] if 'urls' in endpointSet else []
            tcpPorts = endpointSet['tcpPorts'] if 'tcpPorts' in endpointSet else ''
            udpPorts = endpointSet['udpPorts'] if 'udpPorts' in endpointSet else ''
            flatUrls.extend([(category, url, tcpPorts, udpPorts) for url in urls])
    flatIps = []
    for endpointSet in endpointSets:
        if endpointSet['category'] in ('Optimize', 'Allow'):
            ips = endpointSet['ips'] if 'ips' in endpointSet else []
            category = endpointSet['category']
            # IPv4 strings have dots while IPv6 strings have colons
            ip4s = [ip for ip in ips if '.' in ip]
            tcpPorts = endpointSet['tcpPorts'] if 'tcpPorts' in endpointSet else ''
            udpPorts = endpointSet['udpPorts'] if 'udpPorts' in endpointSet else ''
            flatIps.extend([(category, ip, tcpPorts, udpPorts) for ip in ip4s])
    print('IPv4 Firewall IP Address Ranges')
    print(', '.join(sorted(set([ip for (category, ip, tcpPorts, udpPorts) in flatIps]))))
    print('URLs for Proxy Server')
    print(', '.join(sorted(set([url for (category, url, tcpPorts, udpPorts) in flatUrls]))))

    # TODO send mail (e.g. with smtplib/email modules) with new endpoints data
else:
    print('Office 365 worldwide commercial service instance endpoints are up-to-date')

```

Web Service interface versioning

Updates to the parameters or results for these web service methods may be required in the future. After the

general availability version of these web services is published, Microsoft will make reasonable efforts to provide advance notice of material updates to the web service. When Microsoft believes that an update will require changes to clients using the web service, Microsoft will keep the previous version (one version back) of the web service available for at least 12 months after the release of the new version. Customers who do not upgrade during that time may be unable to access the web service and its methods. Customers must ensure that clients of the web service continue working without error if the following changes are made to the web service interface signature:

- Adding a new optional parameter to an existing web method that doesn't have to be provided by older clients and doesn't impact the result an older client receives.
- Adding a new named attribute in one of the response REST items or other columns to the response CSV.
- Adding a new web method with a new name that is not called by the older clients.

Update notifications

You can use a few different methods to get email notifications when changes to the IP addresses and URLs are published to the web service.

- To use a Power Automate solution, see [Use Power Automate to receive an email for changes to Office 365 IP Addresses and URLs](#).
- To deploy an Azure Logic App using an ARM template, see [Office 365 Update Notification \(v1.1\)](#).
- To write your own notification script using PowerShell, see [Send-MailMessage](#).

Exporting a Proxy PAC file

[Get-PacFile](#) is a PowerShell script that reads the latest network endpoints from the Office 365 IP Address and URL web service and creates a sample PAC file. For information on using Get-PacFile, see [Use a PAC file for direct routing of vital Office 365 traffic](#).

Related Topics

[Office 365 URLs and IP address ranges](#)

[Managing Office 365 endpoints](#)

[Office 365 endpoints FAQ](#)

[Office 365 Network Connectivity Principles](#)

[Office 365 network and performance tuning](#)

[Assessing Office 365 network connectivity](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Optimizing your network for Skype for Business Online](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

Other endpoints not included in the Office 365 IP Address and URL Web service

10/28/2022 • 6 minutes to read • [Edit Online](#)

Some network endpoints were previously published and haven't been included in the [Office 365 IP Address and URL Web Service](#). The web service publishes network endpoints that are required for Office 365 connectivity across an enterprise perimeter network. This scope currently doesn't include:

1. Network connectivity that may be required from a Microsoft datacenter to a customer network (inbound hybrid server network traffic).
2. Network connectivity from servers on a customer network across the enterprise perimeter (outbound server network traffic).
3. Uncommon scenarios for network connectivity requirements from a user.
4. DNS resolution connectivity requirement (not listed below).
5. Internet Explorer or Microsoft Edge Trusted Sites.

Apart from DNS, these instances are all optional for most customers unless you need the specific scenario that is described.

ROW	PURPOSE	DESTINATION	TYPE
1	Import Service for PST and file ingestion	Refer to the Import Service for more requirements.	Uncommon outbound scenario
2	Microsoft Support and Recovery Assistant for Office 365	https://autodiscover.outlook.com https://officecdn.microsoft.com https://api.diagnostics.office.com https://apibasic.diagnostics.office.com https://autodiscover-s.outlook.com https://cloudcheckenabler.azurewebsites.net https://login.live.com https://login.microsoftonline.com https://login.windows.net https://o365diagtelemetry.trafficmanager.net https://odc.officeapps.live.com https://offcatedge.azureedge.net https://officeapps.live.com https://outlook.office365.com https://outlookdiagnostics.azureedge.net https://sara.api.support.microsoft.com	Outbound server traffic

ROW	PURPOSE	DESTINATION	TYPE
3	Azure AD Connect (w/SSO option) WinRM & remote PowerShell	Customer STS environment (AD FS Server and AD FS Proxy) TCP ports 80 & 443	Inbound server traffic
4	STS such as AD FS Proxy server(s) (for federated customers only)	Customer STS (such as AD FS Proxy) Ports TCP 443 or TCP 49443 w/ClientTLS	Inbound server traffic
5	Exchange Online Unified Messaging/SBC integration	Bidirectional between on-premises Session Border Controller and *.um.outlook.com	Outbound server-only traffic
6	Mailbox Migration When mailbox migration is initiated from on-premises Exchange Hybrid to Office 365, Office 365 will connect to your published Exchange Web Services (EWS)/Mailbox Replication Services (MRS) server. If you need to allow inbound connections only from specific source IP ranges, create a permit rule for the IP addresses listed in the Exchange Online table in Office 365 URL & IP ranges. To ensure that connectivity to published EWS endpoints (like OWA) is not blocked, make sure the MRS proxy resolves to a separate FQDN and public IP address before you restrict connections.	Customer on-premises EWS/MRS Proxy TCP port 443	Inbound server traffic
7	Exchange Hybrid coexistence functions such as Free/Busy sharing.	Customer on-premises Exchange server	Inbound server traffic
8	Exchange Hybrid proxy authentication	Customer on-premises STS	Inbound server traffic

ROW	PURPOSE	DESTINATION	TYPE
9	Used to configure Exchange Hybrid, using the Exchange Hybrid Configuration Wizard Note: These endpoints are only required to configure Exchange hybrid	domains.live.com on TCP ports 80 & 443, only required for Exchange 2010 SP3 Hybrid Configuration Wizard GCC High, DoD IP addresses: 40.118.209.192/32; 168.62.190.41/32 Worldwide Commercial & GCC: *.store.core.windows.net; asl.configure.office.com; tds.configure.office.com; mshybridservice.trafficmanager.net ; aka.ms/hybridwizard; shcwreleaseprod.blob.core.windows.net/shcw/* ;	Outbound server-only traffic
10	The AutoDetect service is used in Exchange Hybrid scenarios with Hybrid Modern Authentication with Outlook for iOS and Android <email_domain>.outlookmobile.com <email_domain>.outlookmobile.us 52.125.128.0/20 52.127.96.0/23	Customer on-premises Exchange server on TCP 443	Inbound server traffic
11	Exchange hybrid Azure AD authentication	*.msapproxy.net	TCP outbound server-only traffic
12	Skype for Business in Office 2016 includes video based screen sharing, which uses UDP ports. Prior Skype for Business clients in Office 2013 and earlier used RDP over TCP port 443.	TCP port 443 opens to 52.112.0.0/14	Skype for Business older client versions in Office 2013 and earlier
13	Skype for Business hybrid on-premises server connectivity to Skype for Business Online	13.107.64.0/18, 52.112.0.0/14 UDP ports 50,000-59,999 TCP ports 50,000-59,999; 5061	Skype for Business on-premises server outbound connectivity

ROW	PURPOSE	DESTINATION	TYPE
14	Cloud PSTN with on-premises hybrid connectivity requires network connectivity open to the on-premises hosts. For more details about Skype for Business Online hybrid configurations	See Plan hybrid connectivity between Skype for Business Server and Office 365	Skype for Business on-premises hybrid inbound
15	Authentication and identity FQDNs The FQDN <code>secure.aadcdn.microsoftonline-p.com</code> needs to be in your client's Internet Explorer (IE) or Edge Trusted Sites Zone to function.		Trusted Sites
16	Microsoft Teams FQDNs If you are using Internet Explorer or Microsoft Edge, you need to enable first and third-party cookies and add the FQDNs for Teams to your Trusted Sites. This is in addition to the suite-wide FQDNs, CDNs, and telemetry listed in row 14. See Known issues for Microsoft Teams for more information.		Trusted Sites
17	SharePoint Online and OneDrive for Business FQDNs All '.sharepoint.com' FQDNs with '<tenant>' in the FQDN need to be in your client's IE or Edge Trusted Sites Zone to function. In addition to the suite-wide FQDNs, CDNs, and telemetry listed in row 14, you'll need to also add these endpoints.		Trusted Sites

ROW	PURPOSE	DESTINATION	TYPE
18	Yammer Yammer is only available in the browser and requires the authenticated user to be passed through a proxy. All Yammer FQDNs need to be in your client's IE or Edge Trusted Sites Zone to function.		Trusted Sites
19	Use Azure AD Connect to sync on-premises user accounts to Azure AD.	See Hybrid Identity Required Ports and Protocols, Troubleshoot Azure AD connectivity , and Azure AD Connect Health Agent Installation .	Outbound server-only traffic
20	Azure AD Connect with 21 ViaNet in China to sync on-premises user accounts to Azure AD.	*.digicert.com:80 *.entrust.net:80 *.chinacloudapi.cn:443 secure.aadcdn.partner.microsoftonline.cn:443 *.partner.microsoftonline.cn:443 Also see Troubleshoot ingress with Azure AD connectivity issues .	Outbound server-only traffic
21	Microsoft Stream (needs the Azure AD user token). Office 365 Worldwide (including GCC)	*.cloudapp.net *.api.microsoftstream.com *.notification.api.microsoftstream.com amp.azure.net api.microsoftstream.com az416426.vo.msecnd.net s0.assets-yammer.com vortex.data.microsoft.com web.microsoftstream.com TCP port 443	Inbound server traffic
22	Use MFA server for multi-factor authentication requests, both new installations of the server and setting it up with Active Directory Domain Services (AD DS).	See Getting started with the Azure AD multi-factor authentication Server .	Outbound server-only traffic
23	Microsoft Graph Change Notifications Developers can use change notifications to subscribe to events in the Microsoft Graph.	Public Cloud: 52.159.23.209, 52.159.17.84, 52.147.213.251, 52.147.213.181, 13.85.192.59, 13.85.192.123, 20.9.36.45, 20.9.35.166, 20.96.21.67, 20.69.245.215, 137.135.11.161, 137.135.11.116,	Inbound server traffic

ROW	PURPOSE	DESTINATION	TYPE
		52.159.107.50, 52.159.107.4, 52.229.38.131, 52.183.67.212, 52.142.114.29, 52.142.115.31, 51.124.75.43, 51.124.73.177, 20.44.210.83, 20.44.210.146, 40.80.232.177, 40.80.232.118, 20.48.12.75, 20.48.11.201, 104.215.13.23, 104.215.6.169, 52.148.24.136, 52.148.27.39, 40.76.162.99, 40.76.162.42, 40.74.203.28, 40.74.203.27, 20.9.37.73, 20.9.37.76, 20.96.21.98, 20.96.21.115, 137.135.11.222, 137.135.11.250, 52.159.109.205, 52.159.102.72, 52.151.30.78, 52.191.173.85, 51.104.159.213, 51.104.159.181, 51.138.90.7, 51.138.90.52, 52.148.115.48, 52.148.114.238, 40.80.233.14, 40.80.239.196, 20.48.14.35, 20.48.15.147, 104.215.18.55, 104.215.12.254, 20.199.102.157, 20.199.102.73, 13.87.81.123, 13.87.81.35, 20.111.9.46, 20.111.9.77, 13.87.81.133, 13.87.81.141 Microsoft Cloud for US Government: 52.244.33.45, 52.244.35.174, 52.243.157.104, 52.243.157.105, 52.182.25.254, 52.182.25.110, 52.181.25.67, 52.181.25.66, 52.244.111.156, 52.244.111.170, 52.243.147.249, 52.243.148.19, 52.182.32.51, 52.182.32.143, 52.181.24.199, 52.181.24.220 Microsoft Cloud China operated by 21Vianet: 42.159.72.35, 42.159.72.47,	

ROW	PURPOSE	42.159.180.55, DESTINATION, 42.159.180.56, 40.125.138.23, 40.125.136.69, 40.72.155.199, 40.72.155.216 TCP port 443 Note: Developers can specify different ports when creating the subscriptions.	TYPE
24	Network Connection Status Indicator Used by Windows 10 and 11 to determine if the computer is connected to the internet (does not apply to non-Windows clients). When this URL cannot be reached, Windows will assume it is not connected to the Internet and M365 Apps for Enterprise will not try to verify activation status, causing connections to Exchange and other services to fail.	www.msftconnecttest.com 13.107.4.52 Also see Manage connection endpoints for Windows 11 Enterprise and Manage connection endpoints for Windows 10 Enterprise, version 21H2 .	Outbound server-only traffic
25	Teams Notifications on Mobile Devices Used by Android and Apple mobile devices to receive push notifications to the Teams client for incoming calls and other Teams services. When these ports are blocked, all push notifications to mobile devices will fail.	For specific ports, see FCM ports and your firewall in the Google Firebase documentation and If your Apple devices aren't getting Apple push notifications .	Outbound server-only traffic

Related Topics

[Managing Office 365 endpoints](#)

[Monitor Microsoft 365 connectivity](#)

[Client connectivity](#)

[Content delivery networks](#)

[Azure IP Ranges and Service Tags – Public Cloud](#)

[Azure IP Ranges and Service Tags – US Government Cloud](#)

[Azure IP Ranges and Service Tags – Germany Cloud](#)

Azure IP Ranges and Service Tags – China Cloud

Microsoft Public IP Space

Additional network security requirements for Office 365 GCC High and DOD

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to Office 365 GCC High, Office 365 DOD, Microsoft 365 GCC High, and Microsoft 365 DOD.

Office 365 GCC High and DOD are secure cloud environments to meet the needs of the United States Government and its suppliers and contractors. These cloud environments have additional network restrictions on which external endpoints the services are permitted to access.

GCC High and DOD customers planning to use federated identities or hybrid coexistence may require Microsoft to permit inbound and/or outbound access to your existing on-premises deployments. Examples of these activities include:

- Use of federated identities (with Active Directory Federation Services or similar supported STS)
- Hybrid coexistence with an on-premises Exchange Server or Skype for Business deployment
- Migration of existing user content from an on-premises system

To permit the service to communicate with your on-premises endpoints, you **must** send an email to Office 365 engineering for network changes.

WARNING

All requests have a **three-week** SLA and cannot be expedited due to the required security and compliance controls and deployment pipelines. This includes initial onboarding network requests as well as any changes after you have migrated to the service. Make sure that your network teams are aware of this timeline and include it in their planning cycles.

Send an email to [Office 365 Government Allow-List Requests](#) with the following information:

- **To:** [Office 365 Government Allow-List Requests](#)
- **From:** A tenant administrator - the send email **must** match a Global Administrator contact in your tenant
- **Email subject:** Office 365 GCC High Network Request - contoso.onmicrosoft.us (replace with your tenant name)

The body of your message should include the following data:

- Your Microsoft Online Services tenant name (for example, contoso.onmicrosoft.com, fabrikam.onmicrosoft.us)
- An email distribution list that Microsoft will communicate with for on-going communications related to network changes and/or follow up for invalid subnets
- Indicate whether you plan to use Microsoft Teams hybrid coexistence with your on-premises deployments
- Federated identity system externally accessible URL (for example, sts.contoso.com) and IP address range in CIDR notation (for example, 10.1.1.0/28)
- On-Premises PKI Certificate Revocation List URL and IP address range in CIDR notation
- Externally accessible URL and IP address range for Exchange Server on-premises deployment in CIDR notation
- Externally accessible URL and IP address range for Skype for Business on-premises deployment in CIDR notation

For security and compliance reasons, keep in mind the following restrictions on your request:

- There's a four subnet limitation per tenant
- Subnets must be in CIDR Notation (for example, 10.1.1.0/28)
- Subnet ranges can't be larger than /24
- We **cannot** accommodate requests to allow access to commercial cloud services (commercial Office 365, Google G-Suite, Amazon Web Services, etc.)

Once your request has been received and approved by Microsoft, there's a three-week SLA for implementation and can't be expedited. You'll receive an initial acknowledgment when we've received your request and a final acknowledgment once it has been completed.

DNS records for Office 365 DoD

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to Office 365 DoD and Microsoft 365 DoD

As part of onboarding to Office 365 DoD, you will need to add your SMTP and SIP domains to your Online Services tenant. You'll do this using the New-MsolDomain cmdlet in Azure AD PowerShell or use the [Azure Government Portal](#) to start the process of adding the domain and proving ownership.

Once you have your domains added to your tenant and validated, use the following guidance to add the appropriate DNS records for the services below. You may need to modify the below table to fit your organization's needs with respect to the inbound MX record(s) and any existing Exchange Autodiscover record(s) you have in place. We strongly recommend coordinating these DNS records with your messaging team to avoid any outages or mis-delivery of email.

Exchange Online

TYPE	PRIORITY	HOST NAME	POINTS TO ADDRESS OR VALUE	TTL
MX	0	@	<i>tenant</i> .mail.protection.office365.us (see below for more details)	One Hour
TXT	-	@	v=spf1 include:spf.protection.office365.us -all	One Hour
CNAME	-	autodiscover	autodiscover-dod.office365.us	One Hour

Exchange Autodiscover record

If you have Exchange Server on-premises, we recommend leaving your existing record in place while you migrate to Exchange Online, and update that record once you have completed your migration.

Exchange Online MX Record

The MX record value for your accepted domains follows a standard format as noted above:

tenant.mail.protection.office365.us, replacing *tenant* with the first part of your default tenant name.

For example, if your tenant name is contoso.onmicrosoft.us, you'd use **contoso.mail.protection.office365.us** as the value for your MX record.

Skype for Business Online

CNAME records

TYPE	HOST NAME	POINTS TO ADDRESS OR VALUE	TTL
CNAME	sip	sipdir.online.dod.skypeforbusiness.us	One Hour

TYPE	HOST NAME	POINTS TO ADDRESS OR VALUE	TTL
CNAME	lyncdiscover	webdir.online.dod.skypeforbusiness.us	One Hour

SRV records

TYPE	SERVICE	PROTOCOL	PORT	WEIGHT	PRIORITY	NAME	TARGET	TTL
SRV	_sip	_tls	443	1	100	@	sipdir.online.dod.skypeforbusiness.us	One Hour
SRV	_sipfederationtls	_tcp	5061	1	100	@	sipfed.online.dod.skypeforbusiness.us	One Hour

Other DNS records

IMPORTANT

If you have an existing *msoid* CNAME record in your DNS zone, you must **remove** the record from DNS at this time. The *msoid* record is incompatible with Microsoft 365 Enterprise Apps (*formerly Office 365 ProPlus*) and will prevent activation from succeeding.

DNS records for Office 365 GCC High

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to Office 365 GCC High and Microsoft 365 GCC High

As part of onboarding to Office 365 GCC High, you will need to add your SMTP and SIP domains to your Online Services tenant. You'll do this using the New-MSolDomain cmdlet in Azure AD PowerShell or use the [Azure Government Portal](#) to start the process of adding the domain and proving ownership.

Once you have your domains added to your tenant and validated, use the following guidance to add the appropriate DNS records for the services below. You may need to modify the below table to fit your organization's needs with respect to the inbound MX record(s) and any existing Exchange Autodiscover record(s) you have in place. We strongly recommend coordinating these DNS records with your messaging team to avoid any outages or mis-delivery of email.

Exchange Online

TYPE	PRIORITY	HOST NAME	POINTS TO ADDRESS OR VALUE	TTL
MX	0	@	<i>tenant</i> .mail.protection.office365.us (see below for more details)	One Hour
TXT	-	@	v=spf1 include:spf.protection.office365.us -all	One Hour
CNAME	-	autodiscover	autodiscover.office365.us	One Hour

Exchange Autodiscover record

If you have Exchange Server on-premises, we recommend leaving your existing record in place while you migrate to Exchange Online, and update that record once you have completed your migration.

Exchange Online MX Record

The MX record value for your accepted domains follows a standard format as noted above:

tenant.mail.protection.office365.us, replacing *tenant* with the first part of your default tenant name.

For example, if your tenant name is contoso.onmicrosoft.us, you'd use **contoso.mail.protection.office365.us** as the value for your MX record.

Skype for Business Online

CNAME records

TYPE	HOST NAME	POINTS TO ADDRESS OR VALUE	TTL
CNAME	sip	sipdir.online.gov.skypeforbusiness.us	One Hour

TYPE	HOST NAME	POINTS TO ADDRESS OR VALUE	TTL
CNAME	lyncdiscover	webdir.online.gov.skypeforbusiness.us	One Hour

SRV records

TYPE	SERVICE	PROTOCOL	PORT	WEIGHT	PRIORITY	NAME	TARGET	TTL
SRV	_sip	_tls	443	1	100	@	sipdir.online.gov.skypeforbusiness.us	One Hour
SRV	_sipfederationtls	_tcp	5061	1	100	@	sipfed.online.gov.skypeforbusiness.us	One Hour

Other DNS records

IMPORTANT

If you have an existing *msoid* CNAME record in your DNS zone, you must **remove** the record from DNS at this time. The *msoid* record is incompatible with Microsoft 365 Enterprise Apps (*formerly Office 365 ProPlus*) and will prevent activation from succeeding.

Office 365 Content Delivery Network (CDN) Quickstart

10/28/2022 • 3 minutes to read • [Edit Online](#)

You can use the built-in **Office 365 Content Delivery Network (CDN)** to host static assets (images, JavaScript, Stylesheets, WOFF files) to provide better performance for your SharePoint Online pages. The Office 365 CDN improves performance by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. Also, the Office 365 CDN uses the HTTP/2 protocol for improved compression and HTTP pipelining. The Office 365 CDN service is included as part of your SharePoint Online subscription.

For more detailed information guidance see [Use the Office 365 Content Delivery Network \(CDN\) with SharePoint Online](#).

NOTE

The Office 365 CDN is only available to tenants in the production (worldwide) cloud. Tenants in the US Government, China and Germany clouds do not currently support the Office 365 CDN.

Use the Page Diagnostics for SharePoint tool to identify items not in CDN

You can use the **Page Diagnostics for SharePoint tool** browser extension to easily list assets in your SharePoint Online pages that can be added to a CDN origin.

The **Page Diagnostics for SharePoint tool** is a browser extension for the new Microsoft Edge (<https://www.microsoft.com/edge>) and Chrome browsers that analyzes both SharePoint Online modern portal and classic publishing site pages. The tool provides a report for each analyzed page showing how the page performs against a defined set of performance criteria. To install and learn about the Page Diagnostics for SharePoint tool, visit [Use the Page Diagnostics tool for SharePoint Online](#).

When you run the Page Diagnostics for SharePoint tool on a SharePoint Online page, you can click the **Diagnostic Tests** tab to see a list of assets not being hosted by the CDN. These assets will be listed under the heading **Content Delivery Network (CDN) check** as shown in the screenshot below.

Page diagnostics for SharePoint

...

Diagnostic tests Network trace

Attention required

⊗ Large images detected

⊗ Content Delivery Network (CDN) check

⊗ Requests to SharePoint

Improvement opportunities

ⓘ Web parts using Iframes detected

No action required

✓ Page weight under 500 KB

✓ No web parts impacting page load time

NOTE

The Page Diagnostics tool only works for SharePoint Online, and cannot be used on a SharePoint system page.

CDN Overview

The Office 365 CDN is designed to optimize performance for users by distributing frequently accessed objects like images and javascript files over a high-speed global network, reducing page load time and providing access to hosted objects as close as possible to the user. The CDN fetches your assets from a location called an *origin*. An origin can be a SharePoint site, document library or folder that is accessible by a URL.

The Office 365 CDN is separated into two basic types:

- **Public CDN** is designed to be used for JS (JavaScript), CSS (StyleSheets), Web Font File (WOFF, WOFF2) and non-proprietary images like company logos.
- **Private CDN** is designed to be used for images (PNG, JPG, JPEG, etc.).

You can choose to have both public or private origins for your organization. Most organizations will choose to implement a combination of the two. Both public and private options provide similar performance gains, but each has unique attributes and advantages. For more information about public and private CDN origins, see [Choose whether each origin should be public or private](#).

How to enable Public and Private CDN with the default configuration

Before you make changes to the tenant CDN settings, you should verify that it meets compliance, security and privacy policies of your organization.

For more detailed configuration settings, or if you have already enabled CDN and want to add additional locations (origins), please see the section [Set up and configure the Office 365 CDN by using the SharePoint Online Management Shell](#)

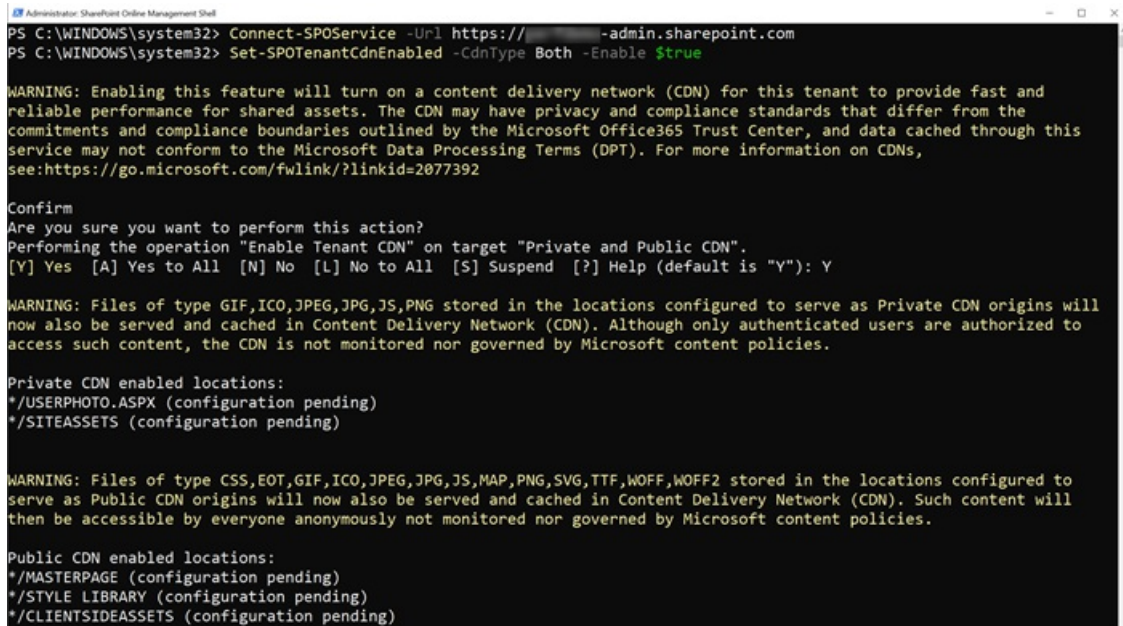
Connect to your tenant using the SharePoint Online Management Shell:

```
Connect-SPOService -Url https://<YourTenantName>-admin.sharepoint.com
```

To enable your organization to use both public and private origins with the default configuration, type the following command:

```
Set-SPOTenantCdnEnabled -CdnType Both -Enable $true
```

Output of these cmdlets should look like the following:



```
Administrator: SharePoint Online Management Shell
PS C:\WINDOWS\system32> Connect-SPOService -Url https://<YourTenantName>-admin.sharepoint.com
PS C:\WINDOWS\system32> Set-SPOTenantCdnEnabled -CdnType Both -Enable $true

WARNING: Enabling this feature will turn on a content delivery network (CDN) for this tenant to provide fast and reliable performance for shared assets. The CDN may have privacy and compliance standards that differ from the commitments and compliance boundaries outlined by the Microsoft Office365 Trust Center, and data cached through this service may not conform to the Microsoft Data Processing Terms (DPT). For more information on CDNs, see:https://go.microsoft.com/fwlink/?linkid=2077392

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable Tenant CDN" on target "Private and Public CDN".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

WARNING: Files of type GIF,ICO,JPEG,JPG,JS,PNG stored in the locations configured to serve as Private CDN origins will now also be served and cached in Content Delivery Network (CDN). Although only authenticated users are authorized to access such content, the CDN is not monitored nor governed by Microsoft content policies.

Private CDN enabled locations:
*/USERPHOTO.ASPX (configuration pending)
*/SITEASSETS (configuration pending)

WARNING: Files of type CSS,EOT,GIF,ICO,JPEG,JPG,JS,MAP,PNG,SVG,TTF,WOFF,WOFF2 stored in the locations configured to serve as Public CDN origins will now also be served and cached in Content Delivery Network (CDN). Such content will then be accessible by everyone anonymously not monitored nor governed by Microsoft content policies.

Public CDN enabled locations:
*/MASTERPAGE (configuration pending)
*/STYLE LIBRARY (configuration pending)
*/CLIENTSIDEASSETS (configuration pending)
```

See also

[Use the Page Diagnostics tool for SharePoint Online](#)

[Use the Office 365 Content Delivery Network \(CDN\) with SharePoint Online](#)

[Content Delivery Networks](#)

[Network planning and performance tuning for Office 365](#)

[SharePoint Performance Series - Office 365 CDN video series](#)

Use the Office 365 Content Delivery Network (CDN) with SharePoint Online

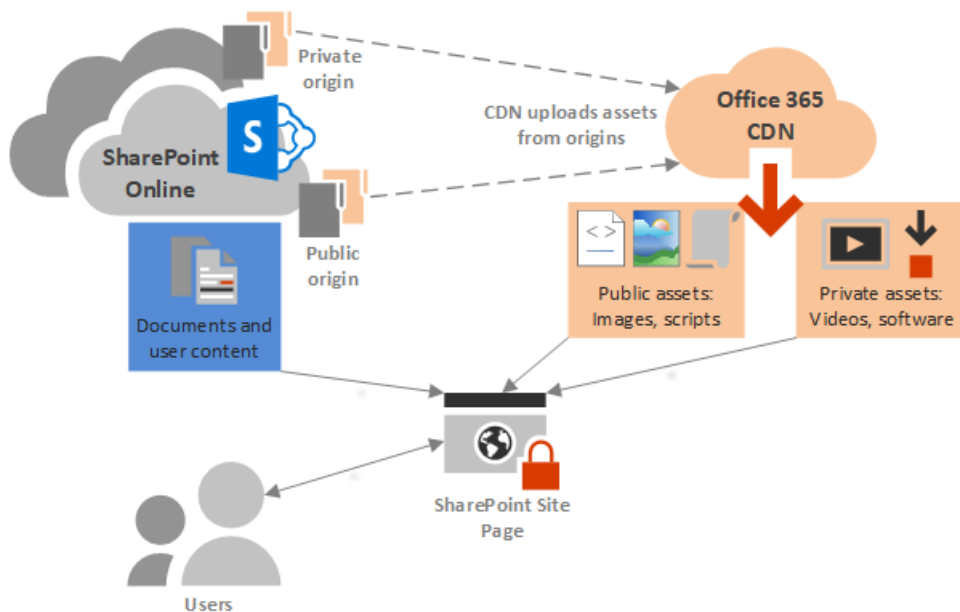
10/28/2022 • 41 minutes to read • [Edit Online](#)

You can use the built-in Office 365 Content Delivery Network (CDN) to host static assets to provide better performance for your SharePoint Online pages. The Office 365 CDN improves performance by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. Also, the Office 365 CDN uses the [HTTP/2 protocol](#) for improved compression and HTTP pipelining. The Office 365 CDN service is included as part of your SharePoint Online subscription.

NOTE

The Office 365 CDN is only available to tenants in the **Production** (worldwide) cloud. Tenants in the US Government and China clouds do not currently support the Office 365 CDN.

The Office 365 CDN is composed of multiple CDNs that allow you to host static assets in multiple locations, or *origins*, and serve them from global high-speed networks. Depending on the kind of content you want to host in the Office 365 CDN, you can add **public** origins, **private** origins or both. See [Choose whether each origin should be public or private](#) for more information on the difference between public and private origins.



If you are already familiar with the way that CDNs work, you only need to complete a few steps to enable the Office 365 CDN for your tenant. This topic describes how. Read on for information about how to get started hosting your static assets.

TIP

There are other Microsoft-hosted CDNs that can be used with Office 365 for specialized usage scenarios, but are not discussed in this topic because they fall outside the scope of the Office 365 CDN. For more information, see [Other Microsoft CDNs](#).

Head back to [Network planning and performance tuning for Office 365](#).

Overview of working with the Office 365 CDN in SharePoint Online

To set up the Office 365 CDN for your organization, you follow these basic steps:

- [Plan for deployment of the Office 365 CDN](#)
 - [Determine which static assets you want to host on the CDN](#).
 - [Determine where you want to store your assets](#). This location can be a SharePoint site, library or folder and is called an *origin*.
 - [Choose whether each origin should be public or private](#). You can add multiple origins of both public and private types.
- Set up and configure the CDN, using either PowerShell or the CLI for Microsoft 365
 - [Set up and configure the CDN by using the SharePoint Online Management Shell](#)
 - [Set up and configure the CDN by using PnP PowerShell](#)
 - [Set up and configure the CDN by using the CLI for Microsoft 365](#)

When you complete this step, you will have:

- Enabled the CDN for your organization.
- Added your origins, identifying each origin as public or private.

Once you're done with setup, you can [Manage the Office 365 CDN](#) over time by:

- Adding, updating, and removing assets
- Adding and removing origins
- Configuring CDN policies
- If necessary, disabling the CDN

Finally, see [Using your CDN assets](#) to learn about accessing your CDN assets from both public and private origins.

See [Troubleshooting the Office 365 CDN](#) for guidance on resolving common issues.

Plan for deployment of the Office 365 CDN

Before you deploy the Office 365 CDN for your Office 365 tenant, you should consider the following factors as part of your planning process.

- [Determine which static assets you want to host on the CDN](#)
- [Determine where you want to store your assets](#)
- [Choose whether each origin should be public or private](#)

Determine which static assets you want to host on the CDN

In general, CDNs are most effective for hosting *static assets*, or assets that don't change very often. A good rule of thumb is to identify files that meet some or all of these conditions:

- Static files embedded in a page (like scripts and images) that may have a significant incremental impact on page load times
- Large files like executables and installation files
- Resource libraries that support client-side code

For example, small files that are repeatedly requested like site images and scripts can significantly improve site rendering performance and incrementally reduce the load on your SharePoint Online sites when you add them

to a CDN origin. Larger files such as installation executables can be downloaded from the CDN, delivering a positive performance impact and subsequent reduction of the load on your SharePoint Online site, even if they are not accessed as often.

Performance improvement on a per-file basis is dependent on many factors, including the client's proximity to the nearest CDN endpoint, transient conditions on the local network, and so forth. Many static files are quite small, and can be downloaded from Office 365 in less than a second. However, a web page may contain many embedded files with a cumulative download time of several seconds. Serving these files from the CDN can significantly reduce the overall page load time. See [What performance gains does a CDN provide?](#) for an example.

Determine where you want to store your assets

The CDN fetches your assets from a location called an *origin*. An origin can be a SharePoint site, document library or folder that is accessible by a URL. You have great flexibility when you specify origins for your organization. For example, you can specify multiple origins or a single origin where you want to put all your CDN assets. You can choose to have both public or private origins for your organization. Most organizations will choose to implement a combination of the two.

You can create new container for your origins such as folders or document libraries, and add files you want to make available from the CDN. This is a good approach if you have a specific set of assets you want to be available from the CDN, and want to restrict the set of CDN assets to only those files in the container.

You can also configure an existing site collection, site, library or folder as an origin, which will make all eligible assets in the container available from the CDN. Before you add an existing container as an origin, it's important to make sure you are aware of its contents and permissions so you do not inadvertently expose assets to anonymous access or unauthorized users.

You can define *CDN policies* to exclude content in your origins from the CDN. CDN policies exclude assets in public or private origins by attributes such as *file type* and *site classification*, and are applied to all origins of the CdnType (private or public) you specify in the policy. For example, if you add a private origin consisting of a site that contains multiple subsites, you can define a policy to exclude sites marked as **Confidential** so content from sites with that classification applied will not be served from the CDN. The policy will apply to content from *all* private origins you have added to the CDN.

Keep in mind that the greater the number of origins, the greater the impact on the time it takes the CDN service to process requests. We recommend that you limit the number of origins as much as possible.

Choose whether each origin should be public or private

When you identify an origin, you specify whether it should be made *public* or *private*. Access to CDN assets in public origins is anonymous, and CDN content in private origins is secured by dynamically generated tokens for greater security. Regardless of which option you choose, Microsoft does all the heavy lifting for you when it comes to administration of the CDN itself. Also, you can change your mind later, after you've set up the CDN and identified your origins.

Both public and private options provide similar performance gains, but each has unique attributes and advantages.

Public origins within the Office 365 CDN are accessible anonymously, and hosted assets can be accessed by anyone who has the URL to the asset. Because access to content in public origins is anonymous, you should only use them to cache non-sensitive generic content such as JavaScript files, scripts, icons and images.

Private origins within the Office 365 CDN provide private access to user content such as SharePoint Online document libraries, sites and proprietary images. Access to content in private origins is secured by dynamically generated tokens so it can only be accessed by users with permissions to the original document library or storage location. Private origins in the Office 365 CDN can only be used for SharePoint Online content, and you

can only access assets in private origins through redirection from your SharePoint Online tenant.

You can read more about how CDN access to assets in a private origin works in [Using assets in private origins](#).

Attributes and advantages of hosting assets in public origins

- Assets exposed in a public origin are accessible by everyone anonymously.

IMPORTANT

You should never place resources that contain user information or are considered sensitive to your organization in a public origin.

- If you remove an asset from a public origin, the asset may continue to be available for up to 30 days from the cache; however, we will invalidate links to the asset in the CDN within 15 minutes.
- When you host style sheets (CSS files) in a public origin, you can use relative paths and URIs within the code. This means that you can reference the location of background images and other objects relative to the location of the asset that's calling it.
- While you can construct a public origin's URL, you should proceed with caution and ensure you utilize the page context property and follow the guidance for doing so. The reason for this is that if access to the CDN becomes unavailable, the URL will not automatically resolve to your organization in SharePoint Online and might result in broken links and other errors. The URL is also subject to change which is why it should not just be hard coded to its current value.
- The default file types that are included for public origins are .css, .eot, .gif, .ico, .jpeg, .jpg, .js, .map, .png, .svg, .ttf, .woff and .woff2. You can specify additional file types.
- You can configure a policy to exclude assets that have been identified by site classifications that you specify. For example, you can choose to exclude all assets that are marked as "confidential" or "restricted" even if they are an allowed file type and are located in a public origin.

Attributes and advantages of hosting assets in private origins

- Private origins can only be used for SharePoint Online assets.
- Users can only access the assets from a private origin if they have permissions to access the container. Anonymous access to these assets is prevented.
- Assets in private origins must be referred from the SharePoint Online tenant. Direct access to private CDN assets does not work.
- If you remove an asset from the private origin, the asset may continue to be available for up to an hour from the cache; however, we will invalidate links to the asset in the CDN within 15 minutes of the asset's removal.
- The default file types that are included for private origins are .gif, .ico, .jpeg, .jpg, .js, and .png. You can specify additional file types.
- Just like with public origins, you can configure a policy to exclude assets that have been identified by site classifications that you specify even if you use wildcards to include all assets within a folder or document library.

For more information about why to use the Office 365 CDN, general CDN concepts, and other Microsoft CDNs you can use with your Office 365 tenant, see [Content Delivery Networks](#).

Default CDN origins

Unless you specify otherwise, Office 365 sets up some default origins for you when you enable the Office 365 CDN. If you initially opt not to provision them, you can add these origins after you complete setup. Unless you

understand the consequences of skipping the setup of default origins and have a specific reason for doing so, you should allow them to be created when you enable the CDN.

Default private CDN origins:

- */siteassets

Default public CDN origins:

- */masterpage
- */style library
- */clientsideassets

NOTE

clientsideassets is a default public origin that was added to the Office 365 CDN service in December 2017. This origin must be present in order for SharePoint Framework solutions in the CDN to work. If you enabled the Office 365 CDN prior to December 2017, or if you skipped setup of default origins when you enabled the CDN, you can manually add this origin. For more information, see [My client-side web part or SharePoint Framework solution isn't working](#).

Set up and configure the Office 365 CDN by using the SharePoint Online Management Shell

The procedures in this section require you to use the SharePoint Online Management Shell to connect to SharePoint Online. For instructions, see [Connect to SharePoint Online PowerShell](#).

Complete these steps to set up and configure the CDN to host your assets in SharePoint Online using the SharePoint Online Management Shell.

► Click to expand

Set up and configure the Office 365 CDN by using PnP PowerShell

The procedures in this section require you to use PnP PowerShell to connect to SharePoint Online. For instructions, see [Getting started with PnP PowerShell](#).

Complete these steps to set up and configure the CDN to host your assets in SharePoint Online using PnP PowerShell.

► Click to expand

Set up and configure the Office 365 CDN using the CLI for Microsoft 365

The procedures in this section require that you have installed the [CLI for Microsoft 365](#). Next, connect to your Office 365 tenant using the [login](#) command.

Complete these steps to set up and configure the CDN to host your assets in SharePoint Online using the CLI for Microsoft 365.

► Click to expand

Using your CDN assets

Now that you have enabled the CDN and configured origins and policies, you can begin using your CDN assets.

This section will help you understand how to use CDN URLs in your SharePoint pages and content so that SharePoint redirects requests for assets in both public and private origins to the CDN.

- [Updating links to CDN assets](#)
- [Using assets in public origins](#)
- [Using assets in private origins](#)

For information on how to use the CDN for hosting client-side web parts, see the topic [Host your client-side web part from Office 365 CDN \(Hello World part 4\)](#).

NOTE

If you add the *ClientSideAssets* folder to the **private** CDN origins list, CDN-hosted custom web parts will fail to render. Files used by SPFX web parts can only utilize the public CDN and the ClientSideAssets folder is a default origin for public CDN.

Updating links to CDN assets

To use assets that you have added to an origin, you simply update links to the original file with the path to the file in the origin.

- Edit the page or content that contains links to assets you have added to an origin. You can also use one of several methods to globally search and replace links across an entire site or site collection if you want to update the link to a given asset everywhere it appears.
- For each link to an asset in an origin, replace the path with the path to the file in the CDN origin. You can use relative paths.
- Save the page or content.

For example, consider the image `/site/SiteAssets/images/image.png`, which you have copied to the document library folder `/site/CDN_origins/public/`. To use the CDN asset, replace the original path to the image file location with the path to the origin to make the new URL `/site/CDN_origins/public/image.png`.

If you want to use the full URL to the asset instead of a relative path, construct the link like so:

```
https://<TenantHostName>.sharepoint.com/sites/site/CDN_origins/public/image.png
```

NOTE

In general, you should not hardcode URLs directly to assets in the CDN. However, you can manually construct URLs for assets in public origins if needed. For more information, see [Hardcoding CDN URLs for public assets](#).

To learn about how to verify that assets are being served from the CDN, see [How do I confirm that assets are being served by the CDN?](#) in [Troubleshooting the Office 365 CDN](#).

Using assets in public origins

The **Publishing feature** in SharePoint Online automatically rewrites URLs of assets stored in public origins to their CDN equivalents so that assets are served from the CDN service instead of SharePoint.

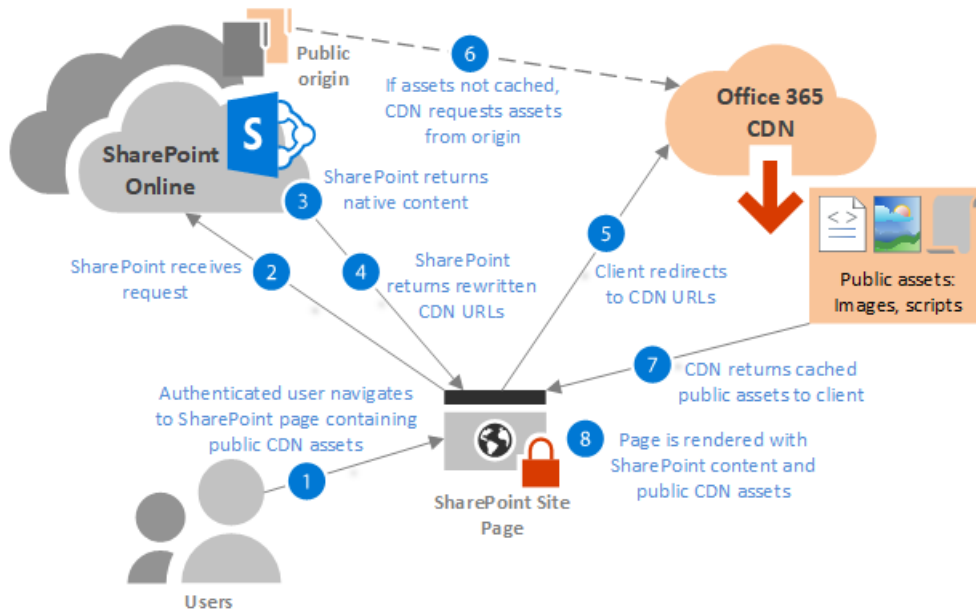
If your origin is in a site with the Publishing feature enabled, and the assets you want to offload to the CDN are in one of the following categories, SharePoint will automatically rewrite URLs for assets in the origin, provided that the asset has not been excluded by a CDN policy.

The following is an overview of which links are automatically rewritten by the SharePoint Publishing feature:

- IMG/LINK/CSS URLs in classic publishing page HTML responses
 - This includes images added by authors within the HTML content of a page

- Picture Library SlideShow webpart image URLs
- Image fields in SPList REST API (RenderListDataAsStream) results
 - Use the new property *ImageFieldsToTryRewriteToCdnUrls* to provide a comma separated list of fields
 - Supports hyperlink fields and PublishingImage fields
- SharePoint image renditions

The following diagram illustrates the workflow when SharePoint receives a request for a page containing assets from a public origin.



TIP

If you want to disable auto-rewriting for specific URLs on a page, you can check out the page and add the query string parameter **?NoAutoReWrites=true** to the end of each link you want to disable.

Constructing CDN URLs for public assets

If the *Publishing* feature is not enabled for a public origin, or the asset is not one of the link types supported by the auto-rewrite feature of the CDN service, you can manually construct URLs to the CDN location of the assets and use these URLs in your content.

NOTE

You cannot hardcode or construct CDN URLs to assets in a private origin because the required access token that forms the last section of the URL is generated at the time the resource is requested. You can construct the URL for Public CDN and the URL should not be hard coded as it is subject to change.

For public CDN assets, the URL format will look like the following:

```
https://publiccdn.sharepointonline.com/<TenantHostName>/sites/site/library/asset.png
```

Replace **TenantHostName** with your tenant name. Example:

```
https://publiccdn.sharepointonline.com/contoso.sharepoint.com/sites/site/library/asset.png
```

NOTE

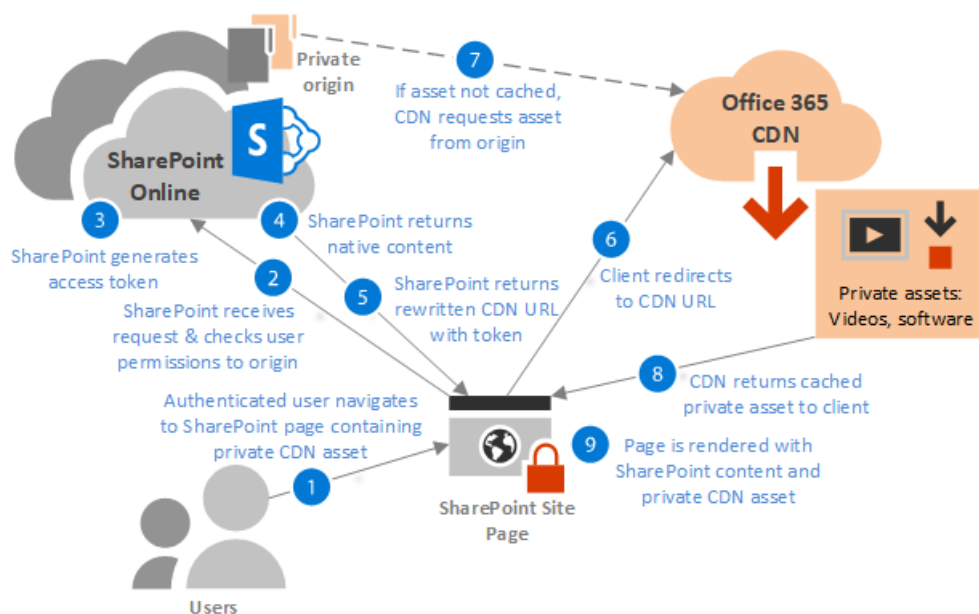
The page context property should be used to construct the prefix instead of hard coding "https://publiccdn.sharepointonline.com". The URL is subject to change and should not be hard coded. If you are using display templates with Classic SharePoint Online then you can use the property "window._spPageContextInfo.publicCdnBaseUrl" in your display template for the prefix of the URL. If you are SPFx web parts for modern and classic SharePoint then you can utilize the property "this.context.pageContext.legacyPageContext.publicCdnBaseUrl". This will provide the prefix so that if it is changed then your implementation will update with it. As an example for SPFx, the URL can be constructed using the property "this.context.pageContext.legacyPageContext.publicCdnBaseUrl" + "/" + "host" + "/" + "relativeURL for the item". Please see [Using CDN in Client-side code](#) which is part of the [season 1 performance series](#)

Using assets in private origins

No additional configuration is required to use assets in private origins. SharePoint Online automatically rewrites URLs for assets in private origins so requests for those assets will always be served from the CDN. You cannot manually build URLs to CDN assets in private origins because these URLs contain tokens that must be auto-generated by SharePoint Online at the time the asset is requested.

Access to assets in private origins is protected by dynamically generated tokens based on user permissions to the origin, with the caveats described in the following sections. Users must have at least **read** access to the origins for the CDN to render content.

The following diagram illustrates the workflow when SharePoint receives a request for a page containing assets from a private origin.



Token-based authorization in private origins

Access to assets in private origins in the Office 365 CDN is granted by tokens generated by SharePoint Online. Users who already have permission to access the folder or library designated by the origin are automatically granted tokens that permit the user to access the file based on their permission level. These access tokens are valid for 30 to 90 minutes after they are generated to help prevent token replay attacks.

Once the access token is generated, SharePoint Online returns a custom URI to the client containing two authorization parameters *eat* (edge authorization token) and *oat* (origin authorization token). The structure of each token is `<'expiration time in Epoch time format'>__<'secure signature'>`. For example:

https://privatecdn.sharepointonline.com/contoso.sharepoint.com/sites/site1/library1/folder1/image1.jpg?eat=1486154359_cc59042c5c55c90b26a2775323c7c8112718431228fe84d568a3795a63912840&oat=1486154359_7d73c2e3ba4b7b1f97242332900616db0d4ffb04312

NOTE

Anyone in possession of the token can access the resource in the CDN. However, URLs containing these access tokens are only shared over HTTPS, so unless the URL is explicitly shared by an end user before the token expires, the asset won't be accessible to unauthorized users.

Item-level permissions are not supported for assets in private origins

It is important to note that SharePoint Online does not support item-level permissions for assets in private origins. For example, for a file located at

`https://contoso.sharepoint.com/sites/site1/library1/folder1/image1.jpg`, users have effective access to the file given the following conditions:

USER	PERMISSIONS	EFFECTIVE ACCESS
User 1	Has access to folder1	Can access image1.jpg from the CDN
User 2	Does not have access to folder1	Cannot access image1.jpg from the CDN
User 3	Does not have access to folder1, but is granted explicit permission to access image1.jpg in SharePoint Online	Can access the asset image1.jpg directly from SharePoint Online, but not from the CDN
User 4	Has access to folder1, but has been explicitly denied access to image1.jpg in SharePoint Online	Cannot access the asset from SharePoint Online, but can access the asset from the CDN despite being denied access to the file in SharePoint Online

Troubleshooting the Office 365 CDN

How do I confirm that assets are being served by the CDN?

Once you have added links to CDN assets to a page, you can confirm that the asset is being served from the CDN by browsing to the page, right clicking on the image once it has rendered and reviewing the image URL.

You can also use your browser's developer tools to view the URL for each asset on a page, or use a third party network trace tool.

NOTE

If you use a network tool such as Fiddler to test your assets outside of rendering the asset from a SharePoint page, you must manually add the referer header "Referer: `https://yourdomain.sharepoint.com`" to the GET request where the URL is the root URL of your SharePoint Online tenant.

You cannot test CDN URLs directly in a web browser because you must have a referrer coming from SharePoint Online. However, if you add the CDN asset URL to a SharePoint page and then open the page in a browser, you will see the CDN asset rendered on the page.

For more information on using the developer tools in the Microsoft Edge browser, see [Microsoft Edge Developer Tools](#).

To watch a short video hosted in the [SharePoint Developer Patterns and Practices YouTube channel](#) demonstrating how to verify that your CDN is working, please see [Verifying your CDN usage and ensuring optimal network connectivity](#).

Why are assets from a new origin unavailable?

Assets in new origins will not immediately be available for use, as it takes time for the registration to propagate through the CDN and for the assets to be uploaded from the origin to CDN storage. The time required for assets to be available in the CDN depends on how many assets and the files sizes.

My client-side web part or SharePoint Framework solution isn't working

When you enable the Office 365 CDN for public origins, the CDN service automatically creates these default origins:

- */MASTERPAGE
- */STYLE LIBRARY
- */CLIENTSIDEASSETS

If the */clientsideassets origin is missing, SharePoint Framework solutions will fail, and no warning or error messages are generated. This origin may be missing either because the CDN was enabled with the - *NoDefaultOrigins* parameter set to **\$true**, or because the origin was manually deleted.

You can check to see which origins are present with the following PowerShell command:

```
Get-SPOTenantCdnOrigins -CdnType Public
```

Or you can check with the Office 365 CLI:

```
spo cdn origin list
```

To add the origin in PowerShell:

```
Add-SPOTenantCdnOrigin -CdnType Public -OriginUrl */CLIENTSIDEASSETS
```

To add the origin in the Office 365 CLI:

```
spo cdn origin add --origin */CLIENTSIDEASSETS
```

What PowerShell modules and CLI shells do I need to work with the Office 365 CDN?

You can choose to work with the Office 365 CDN using either the **SharePoint Online Management Shell** PowerShell module or the **Office 365 CLI**.

- [Getting started with SharePoint Online Management Shell](#)
- [Installing the Office 365 CLI](#)

See also

[Content Delivery Networks](#)

[Network planning and performance tuning for Office 365](#)

Overview: VPN split tunneling for Microsoft 365

10/28/2022 • 15 minutes to read • [Edit Online](#)

NOTE

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

Enterprises have traditionally used VPNs to support secure remote experiences for their users. While core workloads remained on-premises, a VPN from the remote client routed through a datacenter on the corporate network was the primary method for remote users to access corporate resources. To safeguard these connections, enterprises build layers of network security solutions along the VPN paths. This security was built to protect internal infrastructure and to safeguard mobile browsing of external web sites by rerouting traffic into the VPN and then out through the on-premises Internet perimeter. VPNs, network perimeters, and associated security infrastructure were often purpose-built and scaled for a defined volume of traffic, typically with most connectivity being initiated from within the corporate network, and most of it staying within the internal network boundaries.

For quite some time, VPN models where all connections from the remote user device are routed back into the on-premises network (known as *forced tunneling*) were largely sustainable as long as the concurrent scale of remote users was modest and the traffic volumes traversing VPN were low. Some customers continued to use VPN force tunneling as the status quo even after their applications moved from inside the corporate perimeter to public SaaS clouds.

The use of forced tunneled VPNs for connecting to distributed and performance-sensitive cloud applications is suboptimal, but the negative effects have been accepted by some enterprises so as to maintain the security status quo. An example diagram of this scenario can be seen below:

Traditional enterprise connectivity and Internet access

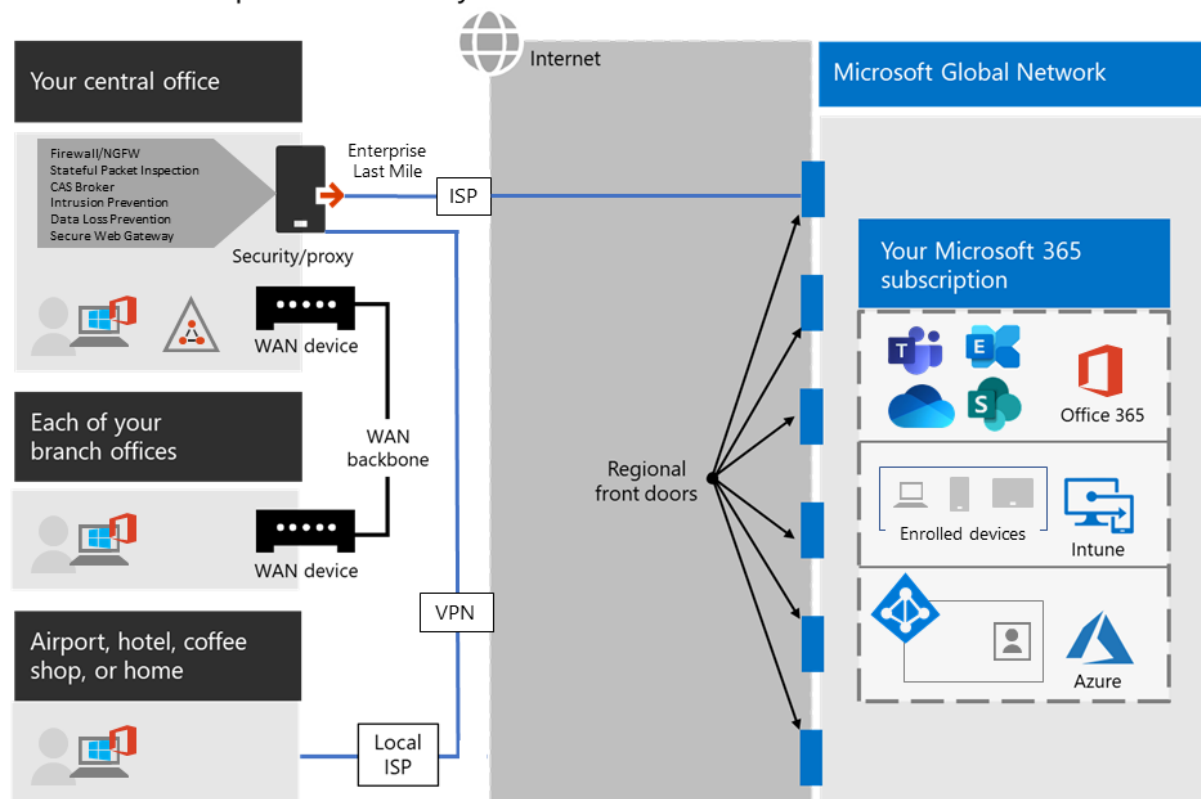


Figure 1: A traditional Forced Tunnel VPN solution.

This problem has been growing for many years, with many customers reporting a significant shift of network traffic patterns. Traffic that used to stay on premises now connects to external cloud endpoints. Many Microsoft customers report that previously, around 80% of their network traffic was to some internal source (represented by the dotted line in the above diagram). In 2020 that number decreased to around 20% or lower as they have shifted major workloads to the cloud. These trends aren't uncommon with other enterprises. Over time, as the cloud journey progresses, the above model becomes increasingly cumbersome and unsustainable, preventing an organization from being agile as they move into a cloud-first world.

The worldwide COVID-19 crisis escalated this problem to require immediate remediation. The need to ensure employee safety has generated unprecedented demands on enterprise IT to support work-from-home productivity at a massive scale. Microsoft 365 is well positioned to help customers fulfill that demand, but high concurrency of users working from home generates a large volume of Microsoft 365 traffic which, if routed through forced tunnel VPN and on-premises network perimeters, causes rapid saturation and runs VPN infrastructure out of capacity. In this new reality, using VPN to access Microsoft 365 is no longer just a performance impediment, but a hard wall that not only impacts Microsoft 365 but critical business operations that still have to rely on the VPN to operate.

Microsoft has been working closely with customers and the wider industry to provide effective, modern solutions to these problems from within our own services, and to align with industry best practice. [Connectivity principles](#) for the Microsoft 365 service have been designed to work efficiently for remote users while still allowing an organization to maintain security and control over their connectivity. These solutions can also be implemented quickly with limited work yet achieve a significant positive effect on the problems outlined above.

For customers who connect their remote worker devices to the corporate network or cloud infrastructure over VPN, Microsoft recommends that the key Microsoft 365 scenarios **Microsoft Teams**, **SharePoint Online**, and **Exchange Online** are routed over a *VPN split tunnel* configuration. This becomes especially important as the first line strategy to facilitate continued employee productivity during large-scale work-from-home events such as the COVID-19 crisis.

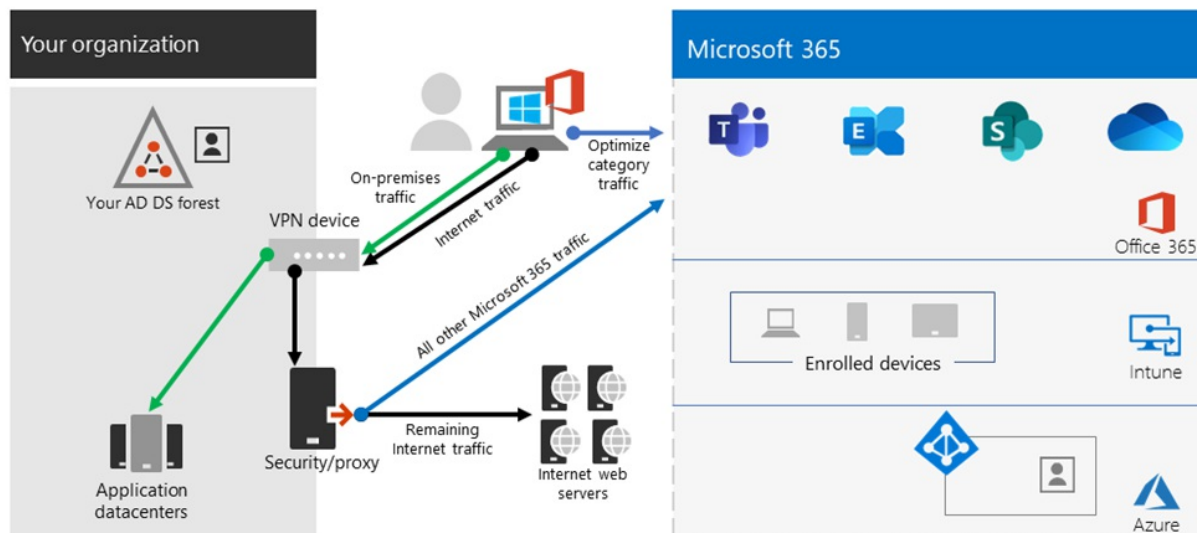


Figure 2: A VPN split tunnel solution with defined Microsoft 365 exceptions sent directly to the service. All other traffic traverses the VPN tunnel regardless of destination.

The essence of this approach is to provide a simple method for enterprises to mitigate the risk of VPN infrastructure saturation and dramatically improve Microsoft 365 performance in the shortest timeframe possible. Configuring VPN clients to allow the most critical, high volume Microsoft 365 traffic to bypass the VPN tunnel achieves the following benefits:

- Immediately mitigates the root cause of a majority of customer-reported performance and network capacity issues in enterprise VPN architectures impacting Microsoft 365 user experience

The recommended solution specifically targets Microsoft 365 service endpoints categorized as **Optimize** in the topic [Microsoft 365 URLs and IP address ranges](#). Traffic to these endpoints is highly sensitive to latency and bandwidth throttling, and enabling it to bypass the VPN tunnel can dramatically improve the end-user experience as well as reduce the corporate network load. Microsoft 365 connections that do not constitute the majority of bandwidth or user experience footprint can continue to be routed through the VPN tunnel along with the rest of the Internet-bound traffic. For more information, see [The VPN split tunnel strategy](#).

- Can be configured, tested, and implemented rapidly by customers and with no additional infrastructure or application requirements

Depending on the VPN platform and network architecture, implementation can take as little as a few hours. For more information, see [Implement VPN split tunneling](#).

- Preserves the security posture of customer VPN implementations by not changing how other connections are routed, including traffic to the Internet

The recommended configuration follows the **least privilege** principle for VPN traffic exceptions and allows customers to implement split tunnel VPN without exposing users or infrastructure to additional security risks. Network traffic routed directly to Microsoft 365 endpoints is encrypted, validated for integrity by Office client application stacks and scoped to IP addresses dedicated to Microsoft 365 services that are hardened at both the application and network level. For more information, see [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios](#) (Microsoft Security Team blog).

- Is natively supported by most enterprise VPN platforms

Microsoft continues to collaborate with industry partners producing commercial VPN solutions to help partners develop targeted guidance and configuration templates for their solutions in alignment with the above recommendations. For more information, see [HOWTO guides for common VPN platforms](#).

TIP

Microsoft recommends focusing split tunnel VPN configuration on documented dedicated IP ranges for Microsoft 365 services. FQDN or AppID-based split tunnel configurations, while possible on certain VPN client platforms, may not fully cover key Microsoft 365 scenarios and may conflict with IP based VPN routing rules. For this reason, Microsoft does not recommend using Microsoft 365 FQDNs to configure split tunnel VPN. The use of FQDN configuration may be useful in other related scenarios, such as .pac file customizations or to implement proxy bypass.

For full implementation guidance, see [Implementing VPN split tunneling for Microsoft 365](#).

For a step-by-step process to configure Microsoft 365 for remote workers, see [Set up your infrastructure for remote work](#)

The VPN split tunnel strategy

Traditional corporate networks are often designed to work securely for a pre-cloud world where most important data, services, applications are hosted on premises and are directly connected to the internal corporate network, as are the majority of users. Thus network infrastructure is built around these elements in that branch offices are connected to the head office via *Multiprotocol Label Switching (MPLS)* networks, and remote users must connect to the corporate network over a VPN to access both on premises endpoints and the Internet. In this model, all traffic from remote users traverses the corporate network and is routed to the cloud service through a common egress point.

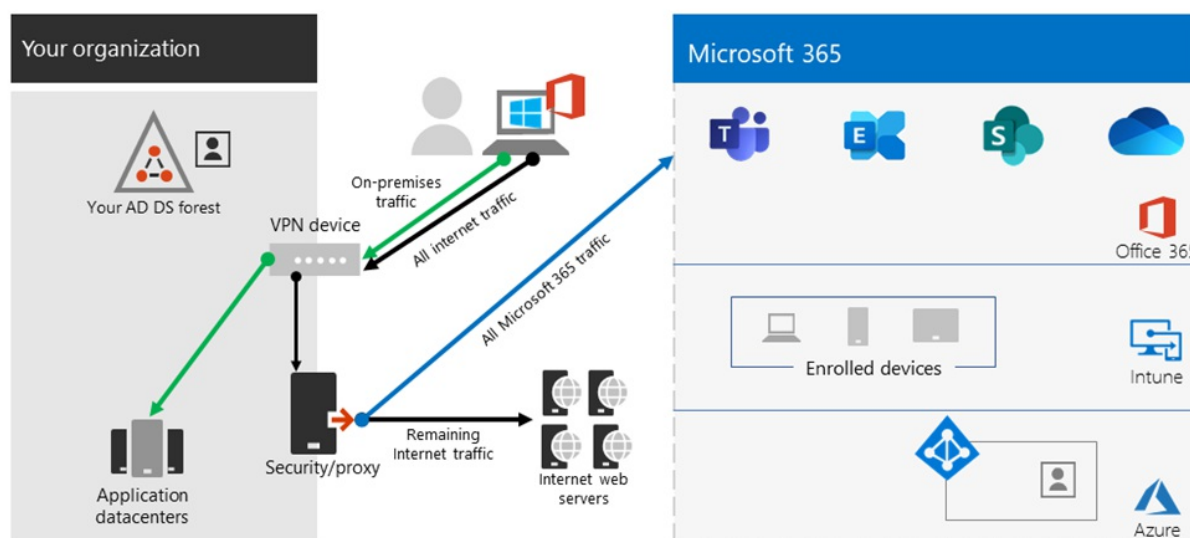


Figure 2: A common VPN solution for remote users where all traffic is forced back into the corporate network regardless of destination

As organizations move data and applications to the cloud, this model has begun to become less effective as it quickly becomes cumbersome, expensive, and unscalable, significantly impacting network performance and efficiency of users and restricting the ability of the organization to adapt to changing needs. Numerous Microsoft customers have reported that a few years ago 80% of network traffic was to an internal destination, but in 2020 80% plus of traffic connects to an external cloud-based resource.

The COVID-19 crisis has aggravated this problem to require immediate solutions for the vast majority of organizations. Many customers have found that the forced VPN model is not scalable or performant enough for 100% remote work scenarios such as that which this crisis has necessitated. Rapid solutions are required for these organizations to continue to operate efficiently.

For the Microsoft 365 service, Microsoft has designed the connectivity requirements for the service with this problem squarely in mind, where a focused, tightly controlled and relatively static set of service endpoints can

be optimized very simply and quickly so as to deliver high performance for users accessing the service, and reducing the burden on the VPN infrastructure so it can be used by traffic that still requires it.

Microsoft 365 categorizes the required endpoints for Microsoft 365 into three categories: **Optimize**, **Allow**, and **Default**. **Optimize** endpoints are our focus here and have the following characteristics:

- Are Microsoft owned and managed endpoints, hosted on Microsoft infrastructure
- Are dedicated to core Microsoft 365 workloads such as Exchange Online, SharePoint Online, Skype for Business Online, and Microsoft Teams
- Have IPs provided
- Low rate of change and are expected to remain small in number (currently 20 IP subnets)
- Are high volume and/or latency sensitive
- Are able to have required security elements provided in the service rather than inline on the network
- Account for around 70-80% of the volume of traffic to the Microsoft 365 service

This tightly scoped set of endpoints can be split out of the forced VPN tunnel and sent securely and directly to the Microsoft 365 service via the user's local interface. This is known as **split tunneling**.

Security elements such as DLP, AV protection, authentication, and access control can all be delivered much more efficiently against these endpoints at different layers within the service. As we also divert the bulk of the traffic volume away from the VPN solution, this frees the VPN capacity up for business critical traffic that still relies on it. It also should remove the need in many cases to go through a lengthy and costly upgrade program to deal with this new way of operating.

VPN Split Tunnel for *Optimize* Microsoft 365 endpoints

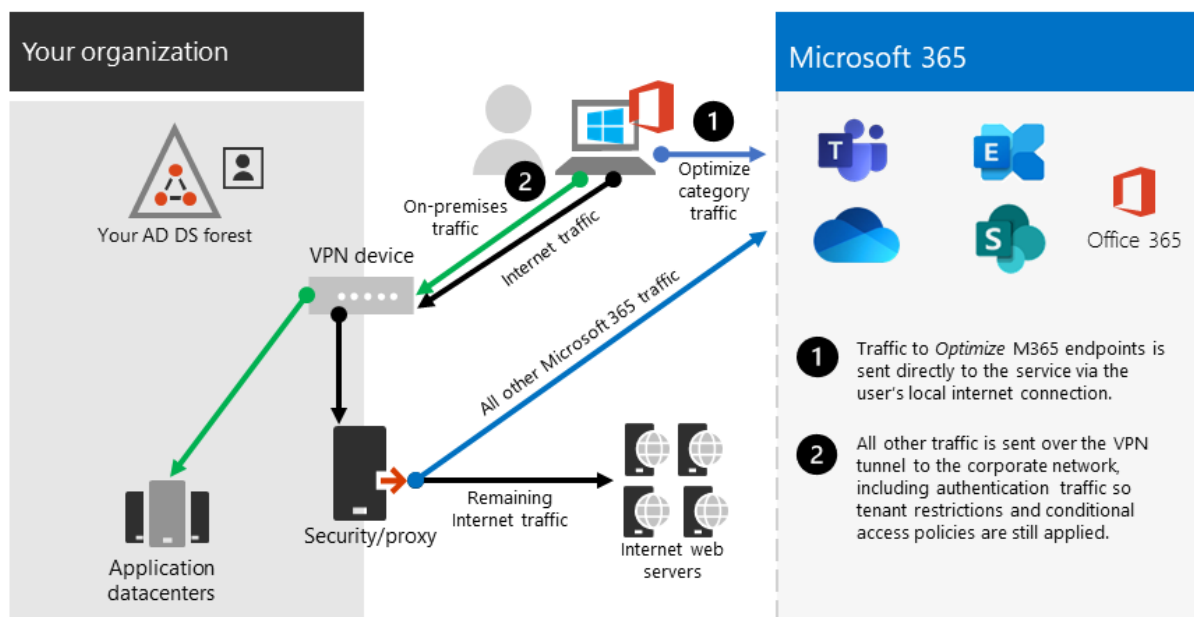


Figure 3: A VPN split tunnel solution with defined Microsoft 365 exceptions sent direct to the service. All other traffic is forced back into the corporate network regardless of destination.

From a security perspective, Microsoft has an array of security features which can be used to provide similar, or even enhanced security than that delivered by inline inspection by on premises security stacks. The Microsoft Security team's blog post [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios](#) has a clear summary of features available and you'll find more detailed guidance within this article. You can also read about Microsoft's implementation of VPN split tunneling at [Running on VPN: How Microsoft is keeping its remote workforce connected](#).

In many cases, this implementation can be achieved in a matter of hours, allowing rapid resolution to one of the most pressing problems facing organizations as they rapidly shift to full scale remote working. For VPN split

tunnel implementation guidance, see [Implementing VPN split tunneling for Microsoft 365](#).

FAQ

The Microsoft Security Team has published [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios](#), a blog post, that outlines key ways for security professionals and IT can achieve modern security controls in today's unique remote work scenarios. In addition, below are some of the common customer questions and answers on this subject.

How do I stop users accessing other tenants I do not trust where they could exfiltrate data?

The answer is a [feature called tenant restrictions](#). Authentication traffic isn't high volume nor especially latency sensitive so can be sent through the VPN solution to the on-premises proxy where the feature is applied. An allow list of trusted tenants is maintained here and if the client attempts to obtain a token to a tenant that isn't trusted, the proxy simply denies the request. If the tenant is trusted, then a token is accessible if the user has the right credentials and rights.

So even though a user can make a TCP/UDP connection to the Optimize marked endpoints above, without a valid token to access the tenant in question, they simply cannot log in and access/move any data.

Does this model allow access to consumer services such as personal OneDrive accounts?

No, it does not, the Microsoft 365 endpoints aren't the same as the consumer services (Onedrive.live.com as an example) so the split tunnel won't allow a user to directly access consumer services. Traffic to consumer endpoints will continue to use the VPN tunnel and existing policies will continue to apply.

How do I apply DLP and protect my sensitive data when the traffic no longer flows through my on-premises solution?

To help you prevent the accidental disclosure of sensitive information, Microsoft 365 has a rich set of [built-in tools](#). You can use the built-in [DLP capabilities](#) of Teams and SharePoint to detect inappropriately stored or shared sensitive information. If part of your remote work strategy involves a bring-your-own-device (BYOD) policy, you can use [app-based Conditional Access](#) to prevent sensitive data from being downloaded to users' personal devices

How do I evaluate and maintain control of the user's authentication when they are connecting directly?

In addition to the tenant restrictions feature noted in Q1, [conditional access policies](#) can be applied to dynamically assess the risk of an authentication request and react appropriately. Microsoft recommends the [Zero Trust model](#) is implemented over time and we can use Azure AD conditional access policies to maintain control in a mobile and cloud-first world. Conditional access policies can be used to make a real-time decision on whether an authentication request is successful based on numerous factors such as:

- Device, is the device known/trusted/Domain joined?
- IP – is the authentication request coming from a known corporate IP address? Or from a country we do not trust?
- Application – Is the user authorized to use this application?

We can then trigger policy such as approve, trigger MFA or block authentication based on these policies.

How do I protect against viruses and malware?

Again, Microsoft 365 provides protection for the Optimize marked endpoints in various layers in the service itself, [outlined in this document](#). As noted, It's vastly more efficient to provide these security elements in the service itself rather than try to do it in line with devices that may not fully understand the protocols/traffic. By default, SharePoint Online [automatically scans file uploads](#) for known malware

For the Exchange endpoints listed above, [Exchange Online Protection](#) and [Microsoft Defender for Microsoft 365](#) do an excellent job of providing security of the traffic to the service.

Can I send more than just the Optimize traffic direct?

Priority should be given to the **Optimize** marked endpoints as these will give maximum benefit for a low level of work. However, if you wish, the **Allow** marked endpoints are required for the service to work and have IP addresses provided for the endpoints that can be used if necessary.

There are also various vendors who offer cloud-based proxy/security solutions called *secure web gateways* which provide central security, control, and corporate policy application for general web browsing. These solutions can work well in a cloud-first world, if highly available, performant, and provisioned close to your users by allowing secure Internet access to be delivered from a cloud-based location close to the user. This removes the need for a hairpin through the VPN/corporate network for general browsing traffic, while still allowing central security control.

Even with these solutions in place however, Microsoft still strongly recommends that Optimize marked Microsoft 365 traffic is sent direct to the service.

For guidance on allowing direct access to an Azure Virtual Network, see [Remote work using Azure VPN Gateway Point-to-site](#).

Why is port 80 required? Is traffic sent in the clear?

Port 80 is only used for things like redirect to a port 443 session, no customer data is sent or is accessible over port 80. [Encryption](#) outlines encryption for data in transit and at rest for Microsoft 365, and [Types of traffic](#) outlines how we use SRTP to protect Teams media traffic.

Does this advice apply to users in China using a worldwide instance of Microsoft 365?

No, it does not. The one caveat to the above advice is users in the PRC who are connecting to a worldwide instance of Microsoft 365. Due to the common occurrence of cross border network congestion in the region, direct Internet egress performance can be variable. Most customers in the region operate using a VPN to bring the traffic into the corporate network and utilize their authorized MPLS circuit or similar to egress outside the country via an optimized path. This is outlined further in the article [Microsoft 365 performance optimization for China users](#).

Does split-tunnel configuration work for Teams running in a browser?

Yes, with caveats. Most Teams functionality is supported in the browsers listed in [Get clients for Microsoft Teams](#).

In addition, Microsoft Edge **96 and above** supports VPN split tunneling for peer-to-peer traffic by enabling the Edge [WebRtcRespectOsRoutingTableEnabled](#) policy. At this time, other browsers may not support VPN split tunneling for peer-to-peer traffic.

Related articles

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Common VPN split tunneling scenarios for Microsoft 365

10/28/2022 • 4 minutes to read • [Edit Online](#)

NOTE

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

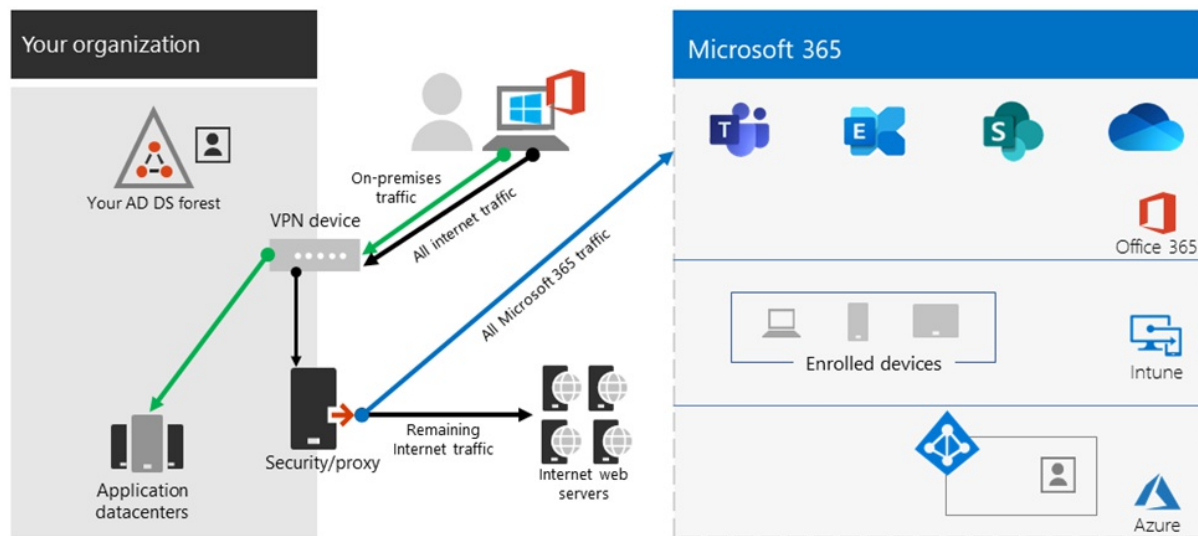
In the list below, you'll see the most common VPN scenarios seen in enterprise environments. Most customers traditionally operate model 1 (VPN Forced Tunnel). This section will help you to quickly and securely transition to **model 2**, which is achievable with relatively little effort, and has enormous benefits to network performance and user experience.

MODEL	DESCRIPTION
1. VPN Forced Tunnel	100% of traffic goes into VPN tunnel, including on-premise, Internet, and all O365/M365
2. VPN Forced Tunnel with few exceptions	VPN tunnel is used by default (default route points to VPN), with few, most important exempt scenarios that are allowed to go direct
3. VPN Forced Tunnel with broad exceptions	VPN tunnel is used by default (default route points to VPN), with broad exceptions that are allowed to go direct (such as all Microsoft 365, All Salesforce, All Zoom)
4. VPN Selective Tunnel	VPN tunnel is used only for corpnet-based services. Default route (Internet and all Internet-based services) goes direct.
5. No VPN	A variation of #2. Instead of legacy VPN, all corpnet services are published through modern security approaches (like Zscaler ZPA, Azure Active Directory (Azure AD) Proxy/MCAS, etc.)

1. VPN Forced Tunnel

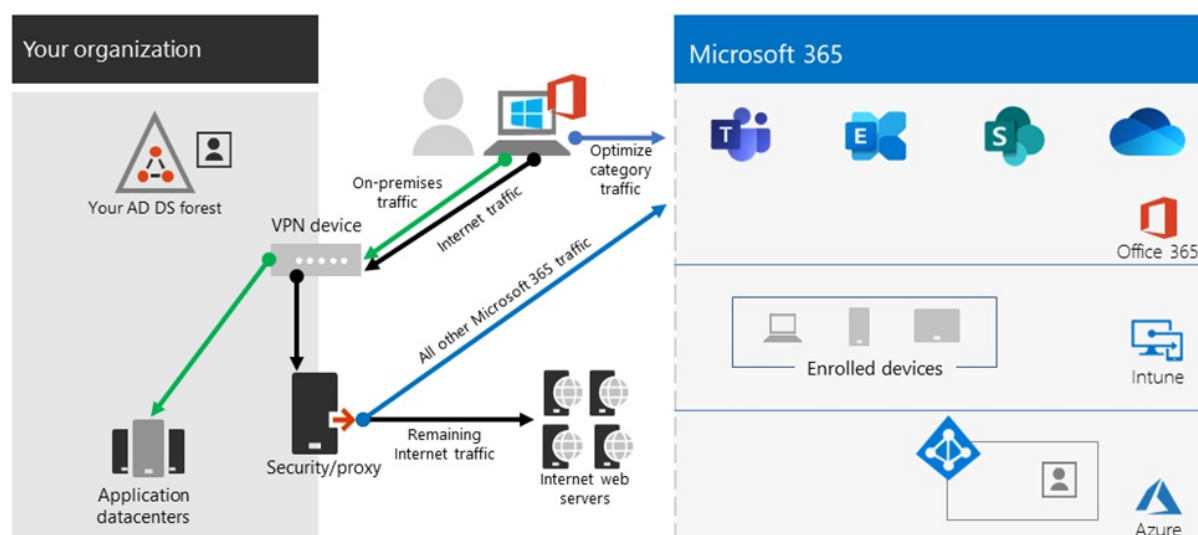
The most common starting scenario for most enterprise customers. A forced VPN is used, which means 100% of

traffic is directed into the corporate network whether the endpoint resides within the corporate network or not. Any external (Internet) bound traffic such as Microsoft 365 or Internet browsing is then hair-pinned back out of the on-premises security equipment such as proxies. In the current climate with nearly 100% of users working remotely, this model therefore puts high load on the VPN infrastructure and is likely to significantly hinder performance of all corporate traffic and thus the enterprise to operate efficiently at a time of crisis.



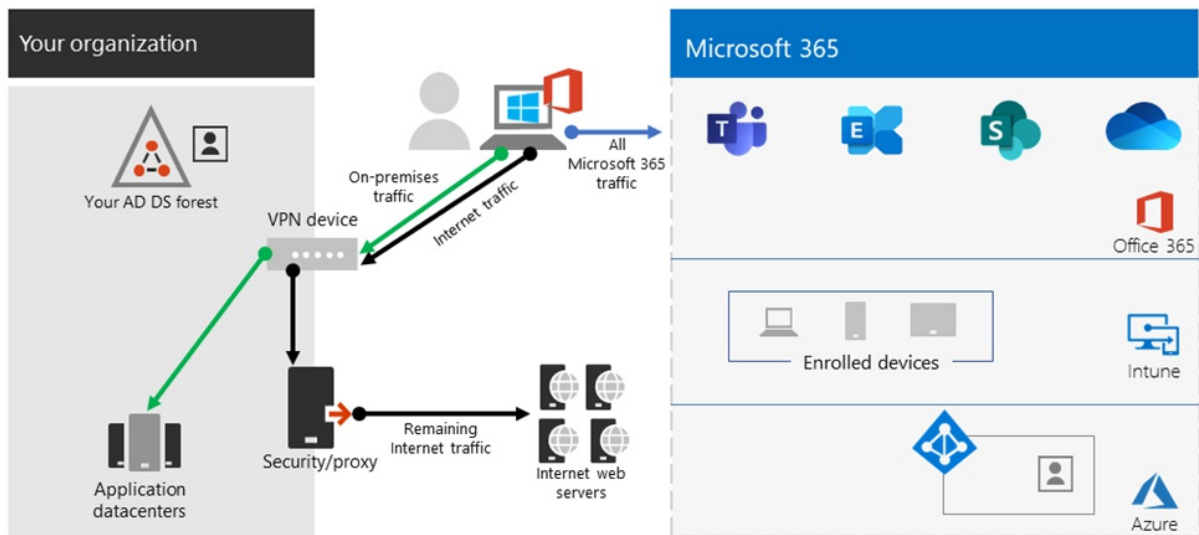
2. VPN Forced Tunnel with a small number of trusted exceptions

Significantly more efficient for an enterprise to operate under. This model allows a few controlled and defined endpoints that are high load and latency sensitive to bypass the VPN tunnel and go direct to the Microsoft 365 service. This significantly improves the performance for the offloaded services, and also decreases the load on the VPN infrastructure, thus allowing elements that still require it to operate with lower contention for resources. It's this model that this article concentrates on assisting with the transition to as it allows for simple, defined actions to be taken quickly with numerous positive outcomes.



3. VPN Forced Tunnel with broad exceptions

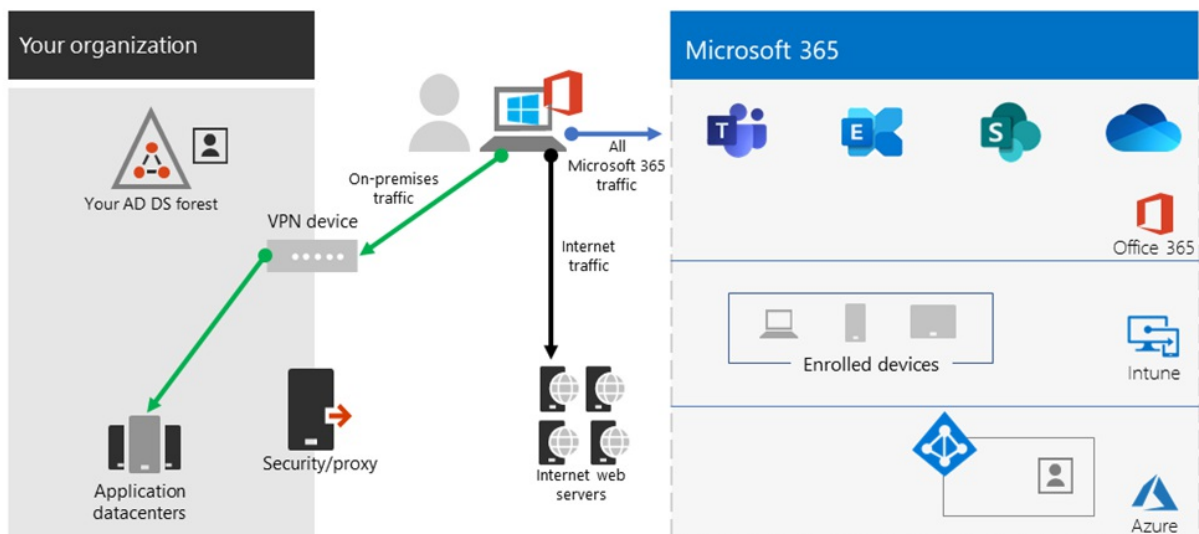
Broadens the scope of model 2. Rather than just sending a small group of defined endpoints direct, it instead sends all traffic directly to trusted services such as Microsoft 365 and Salesforce. This further reduces the load on the corporate VPN infrastructure and improves the performance of the services defined. As this model is likely to take more time to assess the feasibility of and implement, It's likely a step that can be taken iteratively at a later date once model two is successfully in place.



4. VPN selective Tunnel

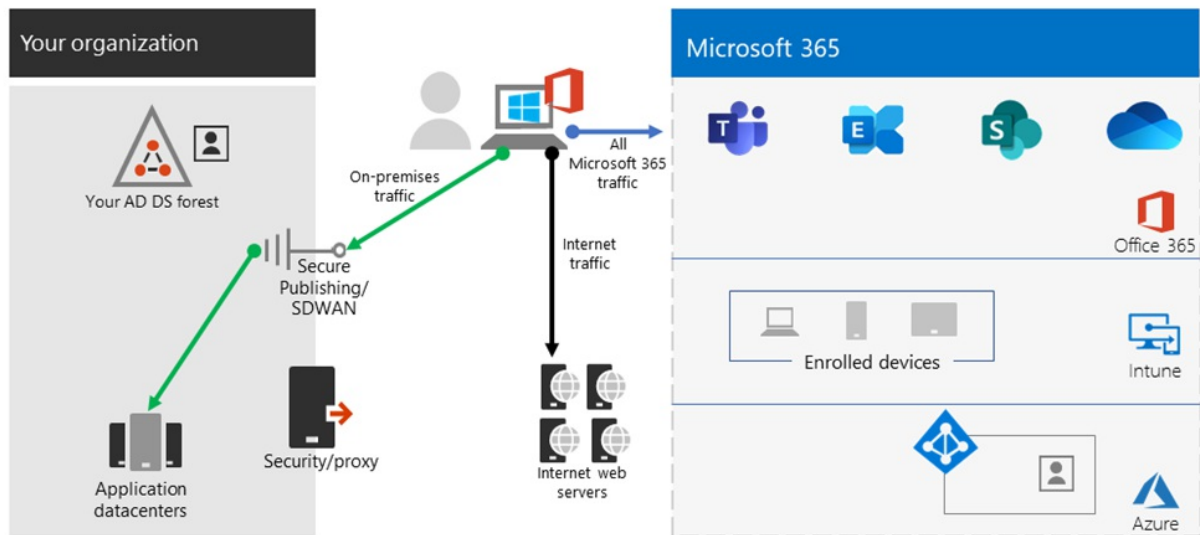
Reverses the third model in that only traffic identified as having a corporate IP address is sent down the VPN tunnel and thus the Internet path is the default route for everything else. This model requires an organization to be well on the path to [Zero Trust](#) in able to safely implement this model. It should be noted that this model or some variation thereof will likely become the necessary default over time as more services move away from the corporate network and into the cloud.

Microsoft uses this model internally. You can find more information on Microsoft's implementation of VPN split tunneling at [Running on VPN: How Microsoft is keeping its remote workforce connected](#).



5. No VPN

A more advanced version of model number 2, whereby any internal services are published through a modern security approach or SDWAN solution such as Azure AD Proxy, Defender for Cloud Apps, Zscaler ZPA, etc.



Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Implementing VPN split tunneling for Microsoft 365

10/28/2022 • 8 minutes to read • [Edit Online](#)

NOTE

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

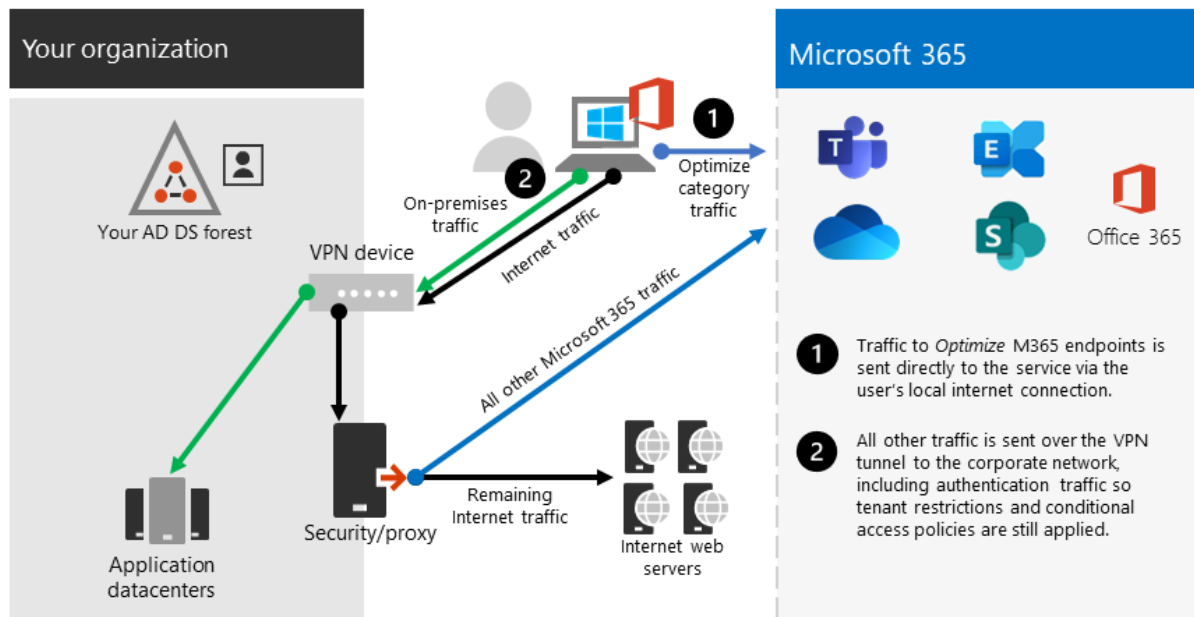
Microsoft's recommended strategy for optimizing remote worker's connectivity is focused on rapidly mitigating problems and providing high performance with a few simple steps. These steps adjust the legacy VPN approach for a few defined endpoints that bypass bottlenecked VPN servers. An equivalent or even superior security model can be applied at different layers to remove the need to secure all traffic at the egress of the corporate network. In most cases, this can be effectively achieved within hours and is then scalable to other workloads as requirements demand and time allows.

Implement VPN split tunneling

In this article, you'll find the simple steps required to migrate your VPN client architecture from a *VPN forced tunnel* to a *VPN forced tunnel with a few trusted exceptions*, [VPN split tunnel model #2](#) in [Common VPN split tunneling scenarios for Microsoft 365](#).

The diagram below illustrates how the recommended VPN split tunnel solution works:

VPN Split Tunnel for *Optimize* Microsoft 365 endpoints



1. Identify the endpoints to optimize

In the [Microsoft 365 URLs and IP address ranges](#) article, Microsoft clearly identifies the key endpoints you need to optimize and categorizes them as **Optimize**. There are currently just four URLs and 20 IP subnets that need to be optimized. This small group of endpoints accounts for around 70% - 80% of the volume of traffic to the Microsoft 365 service including the latency sensitive endpoints such as those for Teams media. Essentially this is the traffic that we need to take special care of and is also the traffic that will put incredible pressure on traditional network paths and VPN infrastructure.

URLs in this category have the following characteristics:

- Are Microsoft owned and managed endpoints, hosted on Microsoft infrastructure
- Have IPs provided
- Low rate of change and are expected to remain small in number (currently 20 IP subnets)
- Are bandwidth and/or latency sensitive
- Are able to have required security elements provided in the service rather than inline on the network
- Account for around 70-80% of the volume of traffic to the Microsoft 365 service

For more information about Microsoft 365 endpoints and how they are categorized and managed, see [Managing Microsoft 365 endpoints](#).

Optimize URLs

The current Optimize URLs can be found in the table below. Under most circumstances, you should only need to use URL endpoints in a [browser PAC file](#) where the endpoints are configured to be sent direct, rather than to the proxy.

OPTIMIZE URLS	PORT/PROTOCOL	PURPOSE
---------------	---------------	---------

OPTIMIZE URLS	PORT/PROTOCOL	PURPOSE
https://outlook.office365.com	TCP 443	This is one of the primary URLs Outlook uses to connect to its Exchange Online server and has a high volume of bandwidth usage and connection count. Low network latency is required for online features including: instant search, other mailbox calendars, free / busy lookup, manage rules and alerts, Exchange online archive, emails departing the outbox.
https://outlook.office.com	TCP 443	This URL is used for Outlook Online Web Access to connect to Exchange Online server, and is sensitive to network latency. Connectivity is particularly required for large file upload and download with SharePoint Online.
<a href="https://<tenant>.sharepoint.com">https://<tenant>.sharepoint.com	TCP 443	This is the primary URL for SharePoint Online and has high-bandwidth usage.
<a href="https://<tenant>-my.sharepoint.com">https://<tenant>-my.sharepoint.com	TCP 443	This is the primary URL for OneDrive for Business and has high bandwidth usage and possibly high connection count from the OneDrive for Business Sync tool.
Teams Media IPs (no URL)	UDP 3478, 3479, 3480, and 3481	Relay Discovery allocation and real-time traffic. These are the endpoints used for Skype for Business and Microsoft Teams Media traffic (calls, meetings, etc.). Most endpoints are provided when the Microsoft Teams client establishes a call (and are contained within the required IPs listed for the service). Use of the UDP protocol is required for optimal media quality.

In the above examples, **tenant** should be replaced with your Microsoft 365 tenant name. For example, **contoso.onmicrosoft.com** would use *contoso.sharepoint.com* and *contoso-my.sharepoint.com*.

Optimize IP address ranges

At the time of writing the IP address ranges that these endpoints correspond to are as follows. It's **very strongly** advised you use a [script such as this](#) example, the [Microsoft 365 IP and URL web service](#) or the [URL/IP page](#) to check for any updates when applying the configuration, and put a policy in place to do so regularly.


```

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16
150.171.32.0/22
150.171.40.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

```

2. Optimize access to these endpoints via the VPN

Now that we have identified these critical endpoints, we need to divert them away from the VPN tunnel and allow them to use the user's local Internet connection to connect directly to the service. The manner in which this is accomplished will vary depending on the VPN product and machine platform used but most VPN solutions will allow some simple configuration of policy to apply this logic. For information VPN platform-specific split tunnel guidance, see [HOWTO guides for common VPN platforms](#).

If you wish to test the solution manually, you can execute the following PowerShell example to emulate the solution at the route table level. This example adds a route for each of the Teams Media IP subnets into the route table. You can test Teams media performance before and after, and observe the difference in routes for the specified endpoints.

Example: Add Teams Media IP subnets into the route table

```

$intIndex = "" # index of the interface connected to the internet
$gateway = "" # default gateway of that interface
$destPrefix = "52.120.0.0/14", "52.112.0.0/14", "13.107.64.0/18" # Teams Media endpoints
# Add routes to the route table
foreach ($prefix in $destPrefix) {New-NetRoute -DestinationPrefix $prefix -InterfaceIndex $intIndex -NextHop $gateway}

```

In the above script, *\$intIndex* is the index of the interface connected to the internet (find by running **get-netadapter** in PowerShell; look for the value of *ifIndex*) and *\$gateway* is the default gateway of that interface (find by running **ipconfig** in a command prompt or **(Get-NetIPConfiguration | Foreach IPv4DefaultGateway).NextHop** in PowerShell).

Once you have added the routes, you can confirm that the route table is correct by running **route print** in a command prompt or PowerShell. The output should contain the routes you added, showing the interface index (22 in this example) and the gateway for that interface (192.168.1.1 in this example):

22	52.120.0.0/14	192.168.1.1	256 4260	ActiveStore
22	52.112.0.0/14	192.168.1.1	256 4260	ActiveStore
22	13.107.64.0/18	192.168.1.1	256 4260	ActiveStore
80	0.0.0.0/0	0.0.0.0	1 55	ActiveStore
22	0.0.0.0/0	192.168.1.1	0 4260	ActiveStore

To add routes for *all* current IP address ranges in the Optimize category, you can use the following script variation to query the [Microsoft 365 IP and URL web service](#) for the current set of Optimize IP subnets and add them to the route table.

Example: Add all Optimize subnets into the route table

```
$intIndex = "" # index of the interface connected to the internet
$gateway = "" # default gateway of that interface
# Query the web service for IPs in the Optimize category
$ep = Invoke-RestMethod ("https://endpoints.office.com/endpoints/worldwide?clientrequestid=" +
([GUID]::NewGuid()).Guid)
# Output only IPv4 Optimize IPs to $optimizeIps
$destPrefix = $ep | where {$_.category -eq "Optimize"} | Select-Object -ExpandProperty ips | Where-Object {
$_ -like '*.*' }
# Add routes to the route table
foreach ($prefix in $destPrefix) {New-NetRoute -DestinationPrefix $prefix -InterfaceIndex $intIndex -NextHop
$gateway}
```

If you inadvertently added routes with incorrect parameters or simply wish to revert your changes, you can remove the routes you just added with the following command:

```
foreach ($prefix in $destPrefix) {Remove-NetRoute -DestinationPrefix $prefix -InterfaceIndex $intIndex -
NextHop $gateway}
```

The VPN client should be configured so that traffic to the **Optimize** IPs are routed in this way. This allows the traffic to utilize local Microsoft resources such as Microsoft 365 Service Front Doors [such as the Azure Front Door](#) that deliver Microsoft 365 services and connectivity endpoints as close to your users as possible. This allows us to deliver high performance levels to users wherever they are in the world and takes full advantage of [Microsoft's world class global network](#), which is likely within a few milliseconds of your users' direct egress.

HOWTO guides for common VPN platforms

This section provides links to detailed guides for implementing split tunneling for Microsoft 365 traffic from the most common partners in this space. We'll add additional guides as they become available.

- **Windows 10 VPN client:** [Optimizing Microsoft 365 traffic for remote workers with the native Windows 10 VPN client](#)
- **Cisco Anyconnect:** [Optimize Anyconnect Split Tunnel for Office365](#)
- **Palo Alto GlobalProtect:** [Optimizing Microsoft 365 Traffic via VPN Split Tunnel Exclude Access Route](#)
- **F5 Networks BIG-IP APM:** [Optimizing Microsoft 365 traffic on Remote Access through VPNs when using BIG-IP APM](#)
- **Citrix Gateway:** [Optimizing Citrix Gateway VPN split tunnel for Office365](#)
- **Pulse Secure:** [VPN Tunneling: How to configure split tunneling to exclude Microsoft 365 applications](#)
- **Check Point VPN:** [How to configure Split Tunnel for Microsoft 365 and other SaaS Applications](#)

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Securing Teams media traffic for VPN split tunneling

10/28/2022 • 5 minutes to read • [Edit Online](#)

NOTE

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

Some Microsoft Teams administrators may require detailed information on how call flows operate in Teams using a split tunneling model and how connections are secured.

Configuration

For both calls and meetings, as long as the required Optimize IP subnets for Teams media are correctly in place in the route table, when Teams calls the [GetBestRoute](#) function to determine which local interface corresponds to the route it should use for a particular destination, the local interface will be returned for Microsoft destinations in the Microsoft IP blocks listed above.

Some VPN client software allows routing manipulation based on URL. However, Teams media traffic has no URL associated with it, so control of routing for this traffic must be done using IP subnets.

In certain scenarios, often unrelated to Teams client configuration, media traffic still traverses the VPN tunnel even with the correct routes in place. If you encounter this scenario, then using a firewall rule to block the Teams IP subnets or ports from using the VPN should suffice.

IMPORTANT

To ensure Teams media traffic is routed via the desired method in all VPN scenarios, please ensure users are running Microsoft Teams client version **1.3.00.13565** or greater. This version includes improvements in how the client detects available network paths.

Signaling traffic is performed over HTTPS and isn't as latency sensitive as the media traffic and is marked as **Allow** in the URL/IP data and thus can safely be routed through the VPN client if desired.

NOTE

Microsoft Edge **96 and above** also supports VPN split tunneling for peer-to-peer traffic. This means customers can gain the benefit of VPN split tunneling for Teams web clients on Edge, for instance. Customers who want to set it up for websites running on Edge can achieve it by taking the additional step of disabling the Edge [WebRtcRespectOsRoutingTableEnabled](#) policy.

Security

One common argument for avoiding split tunnels is that It's less secure to do so, i.e any traffic that does not go through the VPN tunnel won't benefit from whatever encryption scheme is applied to the VPN tunnel, and is therefore less secure.

The main counter-argument to this is that media traffic is already encrypted via *Secure Real-Time Transport Protocol (SRTP)*, a profile of Real-Time Transport Protocol (RTP) that provides confidentiality, authentication, and replay attack protection to RTP traffic. SRTP itself relies on a randomly generated session key, which is exchanged via the TLS secured signaling channel. This is covered in great detail within [this security guide](#), but the primary section of interest is media encryption.

Media traffic is encrypted using SRTP, which uses a session key generated by a secure random number generator and exchanged using the signaling TLS channel. In addition, media flowing in both directions between the Mediation Server and its internal next hop is also encrypted using SRTP.

Skype for Business Online generates username/passwords for secure access to media relays over *Traversal Using Relays around NAT (TURN)*. Media relays exchange the username/password over a TLS-secured SIP channel. It's worth noting that even though a VPN tunnel may be used to connect the client to the corporate network, the traffic still needs to flow in its SRTP form when it leaves the corporate network to reach the service.

Information on how Teams mitigates common security concerns such as voice or *Session Traversal Utilities for NAT (STUN)* amplification attacks can be found in [5.1 Security Considerations for Implementers](#).

You can also read about modern security controls in remote work scenarios at [Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios](#) (Microsoft Security Team blog).

Testing

Once the policy is in place, you should confirm It's working as expected. There are multiple ways of testing the path is correctly set to use the local Internet connection:

- Run the [Microsoft 365 connectivity test](#) that will run connectivity tests for you including trace routes as above. We're also adding in VPN tests into this tooling that should also provide additional insights.
- A simple **tracert** to an endpoint within scope of the split tunnel should show the path taken, for example:

```
tracert worldaz.tr.teams.microsoft.com
```

You should then see a path via the local ISP to this endpoint that should resolve to an IP in the Teams ranges we have configured for split tunneling.

- Take a network capture using a tool such as Wireshark. Filter on UDP during a call and you should see traffic flowing to an IP in the Teams **Optimize** range. If the VPN tunnel is being used for this traffic, then the media traffic won't be visible in the trace.

Additional support logs

If you need further data to troubleshoot, or are requesting assistance from Microsoft support, obtaining the

following information should allow you to expedite finding a solution. Microsoft support's **TSS Windows CMD-based universal TroubleShooting Script toolset** can help you to collect the relevant logs in a simple manner. The tool and instructions on use can be found at <https://aka.ms/TssTools>.

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Special considerations for Stream and live events in VPN environments

10/28/2022 • 15 minutes to read • [Edit Online](#)

NOTE

This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about optimizing Microsoft 365 worldwide tenant performance for users in China, see [Microsoft 365 performance optimization for China users](#).

Microsoft 365 Live Events traffic (this includes attendees to Teams-produced live events and those produced with an external encoder via Teams, Stream, or Yammer) and on-demand Stream traffic is currently categorized as **Default** versus **Optimize** in the [URL/IP list for the service](#). These endpoints are categorized as **Default** because they're hosted on CDNs that may also be used by other services. Customers generally prefer to proxy this type of traffic and apply any security elements normally done on endpoints such as these.

Many customers have asked for URL/IP data needed to connect their users to Stream/Live Events directly from their local internet connection, rather than route the high-volume and latency-sensitive traffic via the VPN infrastructure. Typically, this isn't possible without both dedicated namespaces and accurate IP information for the endpoints, which isn't provided for Microsoft 365 endpoints categorized as **Default**.

Use the following steps to enable direct connectivity for the Stream/Live Events service from clients using a forced tunnel VPN. This solution is intended to provide customers with an option to avoid routing Live Events traffic over VPN while there is high network traffic due to work-from-home scenarios. If possible, it's advised to access the service through an inspecting proxy.

NOTE

Using this solution, there may be service elements that do not resolve to the IP addresses provided and thus traverse the VPN, but the bulk of high-volume traffic like streaming data should. There may be other elements outside the scope of Live Events/Stream which get caught by this offload, but these should be limited as they must meet both the FQDN *and* the IP match before going direct.

IMPORTANT

Customers are advised to weigh the risk of sending more traffic that bypasses the VPN over the performance gain for Live Events.

To implement the forced tunnel exception for Teams Live Events and Stream, the following steps should be applied:

1. Configure external DNS resolution

Clients need external, recursive DNS resolution to be available so that the following host names can be resolved to IP addresses.

- *.azureedge.net
- *.media.azure.net
- *.bmc.cdn.office.net

*.azureedge.net is used for Stream events ([Configure encoders for live streaming in Microsoft Stream - Microsoft Stream | Microsoft Docs](#)).

*.media.azure.net and *.bmc.cdn.office.net are used for Teams-produced Live Events (Quick Start events, RTMP-In supported events [Roadmap ID 84960]) scheduled from the Teams client.

Some of these endpoints are shared with other elements outside of Stream/Live Events, it isn't advised to just use these FQDNs to configure VPN offload even if technically possible in your VPN solution (eg if it works at the FQDN rather than IP).

FQDNs aren't required in the VPN configuration, they are purely for use in PAC files in combination with the IPs to send the relevant traffic direct.

2. Implement PAC file changes (where required)

For organizations that utilize a PAC file to route traffic through a proxy while on VPN, this is normally achieved using FQDNs. However, with Stream/Live Events, the host names provided contain wildcards such as

*.azureedge.net, which also encompasses other elements for which it isn't possible to provide full IP listings. Thus, if the request is sent direct based on DNS wildcard match alone, traffic to these endpoints will be blocked as there is no route via the direct path for it in [Step 3](#) later in this article.

To solve this, we can provide the following IPs and use them in combination with the host names in an example PAC file as described in [Step 1](#). The PAC file checks if the URL matches those used for Stream/Live Events and then if it does, it then also checks to see if the IP returned from a DNS lookup matches those provided for the service. If *both* match, then the traffic is routed direct. If either element (FQDN/IP) doesn't match, then the traffic is sent to the proxy. As a result, the configuration ensures that anything which resolves to an IP outside of the scope of both the IP and defined namespaces will traverse the proxy via the VPN as normal.

Gathering the current lists of CDN Endpoints

Live Events uses multiple CDN providers to stream to customers, to provide the best coverage, quality, and resiliency. Currently, both Azure CDN from Microsoft and from Verizon are used. Over time this could be changed due to situations such as regional availability. This article is a source to enable you to keep up to date on IP ranges.

For Azure CDN from Microsoft, you can download the list from [Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center](#) - you will need to look specifically for the service tag *AzureFrontdoor.Frontend* in the JSON; *addressPrefixes* will show the IPv4/IPv6 subnets. Over time the IPs can change, but the service tag list is always updated before they are put in use.

For Azure CDN from Verizon (Edgecast) you can find an exhaustive list using [Edge Nodes - List](#) (click **Try It**) - you will need to look specifically for the **Premium_Verizon** section. Note that this API shows all Edgecast IPs (origin and Anycast). Currently there isn't a mechanism for the API to distinguish between origin and Anycast.

To implement this in a PAC file you can use the following example which sends the Microsoft 365 Optimize

traffic direct (which is recommended best practice) via FQDN, and the critical Stream/Live Events traffic direct via a combination of the FQDN and the returned IP address. The placeholder name *Contoso* would need to be edited to your specific tenant's name where *contoso* is from contoso.onmicrosoft.com

Example PAC file

Here is an example of how to generate the PAC files:

1. Save the script below to your local hard disk as *Get-TLEPacFile.ps1*.
2. Go to the [Verizon URL](#) and download the resulting JSON (copy paste it into a file like cdnedgenodes.json)
3. Put the file into the same folder as the script.
4. In a PowerShell window, run the following command. Change out the tenant name for something else if you want the SPO URLs. This is Type 2, so **Optimize** and **Allow** (Type 1 is Optimize only).

```
.\Get-TLEPacFile.ps1 -Instance Worldwide -Type 2 -TenantName <contoso> -CdnEdgeNodesFilePath  
.\cdnedgenodes.json -FilePath TLE.pac
```

5. The TLE.pac file will contain all the namespaces and IPs (IPv4/IPv6).

Get-TLEPacFile.ps1

```
# Copyright (c) Microsoft Corporation. All rights reserved.  
# Licensed under the MIT License.  
  
<#PSScriptInfo  
  
.VERSION 1.0.4  
  
.AUTHOR Microsoft Corporation  
  
.GUID 7f692977-e76c-4582-97d5-9989850a2529  
  
.COMPANYNAME Microsoft  
  
.COPYRIGHT  
Copyright (c) Microsoft Corporation. All rights reserved.  
Licensed under the MIT License.  
  
.TAGS PAC Microsoft Microsoft365 365  
  
.LICENSEURI  
  
.PROJECTURI http://aka.ms/ipurlws  
  
.ICONURI  
  
.EXTERNALMODULEDEPENDENCIES  
  
.REQUIREDSCRIPTS  
  
.EXTERNALSCRIPTDEPENDENCIES  
  
.RELEASENOTES  
  
#>  
  
<#  
  
.SYNOPSIS  
  
Create a PAC file for Microsoft 365 prioritized connectivity  
  
.DESCRIPTION
```

This script will access updated information to create a PAC file to prioritize Microsoft 365 Urls for better access to the service. This script will allow you to create different types of files depending on how traffic needs to be prioritized.

.PARAMETER Instance

The service instance inside Microsoft 365.

.PARAMETER ClientRequestId

The client request id to connect to the web service to query up to date Urls.

.PARAMETER DirectProxySettings

The direct proxy settings for priority traffic.

.PARAMETER DefaultProxySettings

The default proxy settings for non priority traffic.

.PARAMETER Type

The type of prioritization to give. Valid values are 1 and 2, which are 2 different modes of operation. Type 1 will send Optimize traffic to the direct route. Type 2 will send Optimize and Allow traffic to the direct route.

.PARAMETER Lowercase

Flag this to include lowercase transformation into the PAC file for the host name matching.

.PARAMETER TenantName

The tenant name to replace wildcard Urls in the webservice.

.PARAMETER ServiceAreas

The service areas to filter endpoints by in the webservice.

.PARAMETER FilePath

The file to print the content to.

.EXAMPLE

```
Get-TLEPacFile.ps1 -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7 -DefaultProxySettings "PROXY 4.4.4.4:70" -FilePath type1.pac
```

.EXAMPLE

```
Get-TLEPacFile.ps1 -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7 -Instance China -Type 2 -DefaultProxySettings "PROXY 4.4.4.4:70" -FilePath type2.pac
```

.EXAMPLE

```
Get-TLEPacFile.ps1 -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7 -Instance WorldWide -Lowercase -TenantName tenantName -ServiceAreas Sharepoint
```

#>

#Requires -Version 2

```
[CmdletBinding(SupportsShouldProcess=$True)]
```

```
Param (
```

```
    [Parameter(Mandatory = $false)]
```

```
    [ValidateSet('Worldwide', 'Germany', 'China', 'USGovDoD', 'USGovGCCHigh')]
```

```
    [String] $Instance = "Worldwide",
```

```
    [Parameter(Mandatory = $false)]
```

```

[ValidateNotNullOrEmpty()]
[guid] $ClientRequestId = [Guid]::NewGuid().Guid,

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[String] $DirectProxySettings = 'DIRECT',

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[String] $DefaultProxySettings = 'PROXY 10.10.10.10:8080',

[Parameter(Mandatory = $false)]
[ValidateRange(1, 2)]
[int] $Type = 1,

[Parameter(Mandatory = $false)]
[switch] $Lowercase = $false,

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[string] $TenantName,

[Parameter(Mandatory = $false)]
[ValidateSet('Exchange', 'SharePoint', 'Common', 'Skype')]
[string[]] $ServiceAreas,

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[string] $FilePath,

[Parameter(Mandatory = $false)]
[ValidateNotNullOrEmpty()]
[string] $CdnEdgeNodesFilePath
)

#####
#####
### Global constants
#####
#####

$baseServiceUrl = "https://endpoints.office.com/endpoints/$Instance/?ClientRequestId={$ClientRequestId}"
$directProxyVarName = "direct"
$defaultProxyVarName = "proxyServer"
$b1 = "`r`n"

#####
#####
### Functions to create PAC files
#####
#####

function Get-PacClauses
{
    param(
        [Parameter(Mandatory = $false)]
        [string[]] $Urls,

        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [String] $ReturnVarName
    )

    if (!$Urls)
    {
        return ""
    }

    $clauses = (($Urls | ForEach-Object { "shExpMatch(host, `"$$_`")" }) -Join "$b1" || ")

```

```

@"
    if($clauses)
    {
        return $ReturnVarName;
    }
"@
}

function Get-PacString
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [array[]] $MapVarUrls
    )

    @"
// This PAC file will provide proxy config to Microsoft 365 services
// using data from the public web service for all endpoints
function FindProxyForURL(url, host)
{
    var $directProxyVarName = "$DirectProxySettings";
    var $defaultProxyVarName = "$DefaultProxySettings";

$( if ($Lowercase) { "    host = host.toLowerCase();" })

$( ($MapVarUrls | ForEach-Object { Get-PACClauses -ReturnVarName $_.Item1 -Urls $_.Item2 }) -Join "$bl$bl" )

$( if (!$ServiceAreas -or $ServiceAreas.Contains('Skype')) { Get-TLEPacConfiguration })

    return $defaultProxyVarName;
}
"@ -replace "($bl){3,}", "$bl$bl" # Collapse more than one blank line in the PAC file so it looks better.
}

#####
####
### Functions to get and filter endpoints
#####

function Get-TLEPacConfiguration {
    param ()
    $PreBlock = @"
// Don't Proxy Teams Live Events traffic

if(shExpMatch(host, "*.azureedge.net")
|| shExpMatch(host, "*.bmc.cdn.office.net")
|| shExpMatch(host, "*.media.azure.net"))
{
    var resolved_ip = dnsResolveEx(host);

"@
    $TLESb = New-Object 'System.Text.StringBuilder'
    $TLESb.Append($PreBlock) | Out-Null

    if (![string]::IsNullOrEmpty($CdnEdgeNodesFilePath) -and (Test-Path -Path $CdnEdgeNodesFilePath)) {
        $CdnData = Get-Content -Path $CdnEdgeNodesFilePath -Raw -ErrorAction SilentlyContinue | ConvertFrom-
Json | Select-Object -ExpandProperty value |
        Where-Object { $_.name -eq 'Premium_Verizon' } | Select-Object -First 1 -ExpandProperty
properties |
        Select-Object -ExpandProperty ipAddressGroups
        $CdnData | Select-Object -ExpandProperty ipv4Addresses | ForEach-Object {
            if ($TLESb.Length -eq $PreBlock.Length) {
                $TLESb.Append("        if(") | Out-Null
            }
        }
        else {
            $TLESb.AppendLine() | Out-Null
        }
    }
}

```

```

        $TLESb.Append("        || ") | Out-Null
    }
    $TLESb.Append("isInNetEx(resolved_ip, `"$($_.BaseIpAddress)/$(_.prefixLength)`")") | Out-Null
}
$CdnData | Select-Object -ExpandProperty ipv6Addresses | ForEach-Object {
    if ($TLESb.Length -eq $PreBlock.Length) {
        $TLESb.Append("        if(") | Out-Null
    }
    else {
        $TLESb.AppendLine() | Out-Null
        $TLESb.Append("        || ") | Out-Null
    }
    $TLESb.Append("isInNetEx(resolved_ip, `"$($_.BaseIpAddress)/$(_.prefixLength)`")") | Out-Null
}
}
$AzureIPsUrl = Invoke-WebRequest -Uri "https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519" -UseBasicParsing -ErrorAction SilentlyContinue |
    Select-Object -ExpandProperty Links | Select-Object -ExpandProperty href |
    Where-Object { $_.EndsWith('.json') -and $_ -match 'ServiceTags' } | Select-Object -First 1
if ($AzureIPsUrl) {
    Invoke-RestMethod -Uri $AzureIPsUrl -ErrorAction SilentlyContinue | Select-Object -ExpandProperty
values |
    Where-Object { $_.name -eq 'AzureFrontDoor.Frontend' } | Select-Object -First 1 -ExpandProperty
properties |
    Select-Object -ExpandProperty addressPrefixes | ForEach-Object {
        if ($TLESb.Length -eq $PreBlock.Length) {
            $TLESb.Append("        if(") | Out-Null
        }
        else {
            $TLESb.AppendLine() | Out-Null
            $TLESb.Append("        || ") | Out-Null
        }
        $TLESb.Append("isInNetEx(resolved_ip, `"$$_`")") | Out-Null
    }
}
if ($TLESb.Length -gt $PreBlock.Length) {
    $TLESb.AppendLine("") | Out-Null
    $TLESb.AppendLine("        {") | Out-Null
    $TLESb.AppendLine("            return $directProxyVarName;") | Out-Null
    $TLESb.AppendLine("        }") | Out-Null
}
else {
    $TLESb.AppendLine("        // no addresses found for service via script") | Out-Null
}
$TLESb.AppendLine("    }") | Out-Null
return $TLESb.ToString()
}

function Get-Regex
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [string] $Fqdn
    )

    return "^" + $Fqdn.Replace(".", "\.").Replace("*", ".").Replace("?", ".?") + "$"
}

function Match-RegexList
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [string] $ToMatch,

        [Parameter(Mandatory = $false)]
        [string[]] $MatchList
    )
}

```

```

    if (!$MatchList)
    {
        return $false
    }
    foreach ($regex in $MatchList)
    {
        if ($regex -ne $ToMatch -and $ToMatch -match (Get-Regex $regex))
        {
            return $true
        }
    }
    return $false
}

function Get-Endpoints
{
    $url = $baseServiceUrl
    if ($TenantName)
    {
        $url += "&TenantName=$TenantName"
    }
    if ($ServiceAreas)
    {
        $url += "&ServiceAreas=" + ($ServiceAreas -Join ",")
    }
    return Invoke-RestMethod -Uri $url
}

function Get-Urls
{
    param(
        [Parameter(Mandatory = $false)]
        [psobject[]] $Endpoints
    )

    if ($Endpoints)
    {
        return $Endpoints | Where-Object { $_.urls } | ForEach-Object { $_.urls } | Sort-Object -Unique
    }
    return @()
}

function Get-UrlVarTuple
{
    param(
        [Parameter(Mandatory = $true)]
        [ValidateNotNullOrEmpty()]
        [string] $VarName,

        [Parameter(Mandatory = $false)]
        [string[]] $Urls
    )
    return New-Object 'Tuple[string,string[]]'($VarName, $Urls)
}

function Get-MapVarUrls
{
    Write-Verbose "Retrieving all endpoints for instance $Instance from web service."
    $Endpoints = Get-Endpoints

    if ($Type -eq 1)
    {
        $directUrls = Get-Urls ($Endpoints | Where-Object { $_.category -eq "Optimize" })
        $nonDirectPriorityUrls = Get-Urls ($Endpoints | Where-Object { $_.category -ne "Optimize" }) |
Where-Object { Match-RegexList $_ $directUrls }
        return @(
            Get-UrlVarTuple -VarName $defaultProxyVarName -Urls $nonDirectPriorityUrls
            Get-UrlVarTuple -VarName $directProxyVarName -Urls $directUrls
        )
    }
}

```

```

        Get-UrlVarTuple -VarName $defaultProxyVarName -Urls $directUrls
    )
}
elseif ($Type -eq 2)
{
    $directUrls = Get-Urls ($Endpoints | Where-Object { $_.category -in @("Optimize", "Allow")})
    $nonDirectPriorityUrls = Get-Urls ($Endpoints | Where-Object { $_.category -notin @("Optimize",
"Allow") }) | Where-Object { Match-RegexList $_ $directUrls }
    return @(
        Get-UrlVarTuple -VarName $defaultProxyVarName -Urls $nonDirectPriorityUrls
        Get-UrlVarTuple -VarName $directProxyVarName -Urls $directUrls
    )
}
}

#####
#####
### Main script
#####
#####

$content = Get-PacString (Get-MapVarUrls)

if ($FilePath)
{
    $content | Out-File -FilePath $FilePath -Encoding ascii
}
else
{
    $content
}

```

The script will automatically parse the Azure list based on the [download URL](#) and keys off of **AzureFrontDoor.Frontend**, so there is no need to get that manually.

Again, it isn't advised to perform VPN offload using just the FQDNs; utilizing **both** the FQDNs and the IP addresses in the function helps scope the use of this offload to a limited set of endpoints including Live Events/Stream. The way the function is structured will result in a DNS lookup being done for the FQDN that matches those listed by the client directly, i.e. DNS resolution of the remaining namespaces remains unchanged.

If you wish to limit the risk of offloading endpoints not related to Live Events and Stream, you can remove the *.azureedge.net domain from the configuration which is where most of this risk lies as this is a shared domain used for all Azure CDN customers. The downside of this is that any event using an external encoder won't be optimized but events produced/organized within Teams will be.

3. Configure routing on the VPN to enable direct egress

The final step is to add a direct route for the Live Event IPs described in **Gathering the current lists of CDN Endpoints** into the VPN configuration to ensure the traffic isn't sent via the forced tunnel into the VPN. Detailed information on how to do this for Microsoft 365 Optimize endpoints can be found in the [Implement VPN split tunneling](#) section of [Implementing VPN split tunneling for Microsoft 365](#). The process is exactly the same for the Stream/Live Events IPs listed in this document.

Note that only the IPs (not FQDNs) from [Gathering the current lists of CDN Endpoints](#) should be used for VPN configuration.

FAQ

Will this send all my traffic to the service direct?

No, this will send the latency-sensitive streaming traffic for a Live Event or Stream video direct, any other traffic will continue to use the VPN tunnel if they do not resolve to the IPs published.

Do I need to use the IPv6 Addresses?

No, the connectivity can be IPv4 only if required.

Why are these IPs not published in the Microsoft 365 URL/IP service?

Microsoft has strict controls around the format and type of information that is in the service to ensure customers can reliably use the information to implement secure and optimal routing based on endpoint category.

The **Default** endpoint category has no IP information provided for numerous reasons (Default endpoints may be outside of the control of Microsoft, may change too frequently, or may be in blocks shared with other elements). For this reason, Default endpoints are designed to be sent via FQDN to an inspecting proxy, like normal web traffic.

In this case, the above endpoints are CDNs that may be used by non-Microsoft controlled elements other than Live Events or Stream, and thus sending the traffic direct will also mean anything else which resolves to these IPs will also be sent direct from the client. Due to the unique nature of the current global crisis and to meet the short-term needs of our customers, Microsoft has provided the information above for customers to use as they see fit.

Microsoft is working to reconfigure the Live Events endpoints to allow them to be included in the Allow/Optimize endpoint categories in the future.

Do I only need to allow access to these IPs?

No, access to all of the **Required** marked endpoints in [the URL/IP service](#) is essential for the service to operate. In addition, any Optional endpoint marked for Stream (ID 41-45) is required.

What scenarios will this advice cover?

1. Live events produced within the Teams App
2. Viewing Stream hosted content
3. External device (encoder) produced events

Does this advice cover presenter traffic?

It does not, the advice above is purely for those consuming the service. Presenting from within Teams will see the presenter's traffic flowing to the Optimize marked UDP endpoints listed in URL/IP service row 11 with detailed VPN offload advice outlined in the [Implement VPN split tunneling](#) section of [Implementing VPN split tunneling for Microsoft 365](#).

Does this configuration risk traffic other than Live Events & Stream being sent direct?

Yes, due to shared FQDNs used for some elements of the service, this is unavoidable. This traffic is normally sent via a corporate proxy which can apply inspection. In a VPN split tunnel scenario, using both the FQDNs and IPs will scope this risk down to a minimum, but it will still exist. Customers can remove the ***.azureedge.net** domain from the offload configuration and reduce this risk to a bare minimum but this will remove the offload of Stream-supported Live Events (Teams-scheduled, external encoder events, Yammer events produced in Teams, Yammer-scheduled external encoder events, and Stream scheduled events or on-demand viewing from Stream). Events scheduled and produced in Teams are unaffected.

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Microsoft 365 performance optimization for China users](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Microsoft 365 global tenant performance optimization for China users

10/28/2022 • 8 minutes to read • [Edit Online](#)

IMPORTANT

This guidance is specific to usage scenarios in which **enterprise Microsoft 365 users located in China** connect to a **global Microsoft 365 tenant**. This guidance does **not** apply to tenants in Office 365 operated by 21Vianet.

NOTE

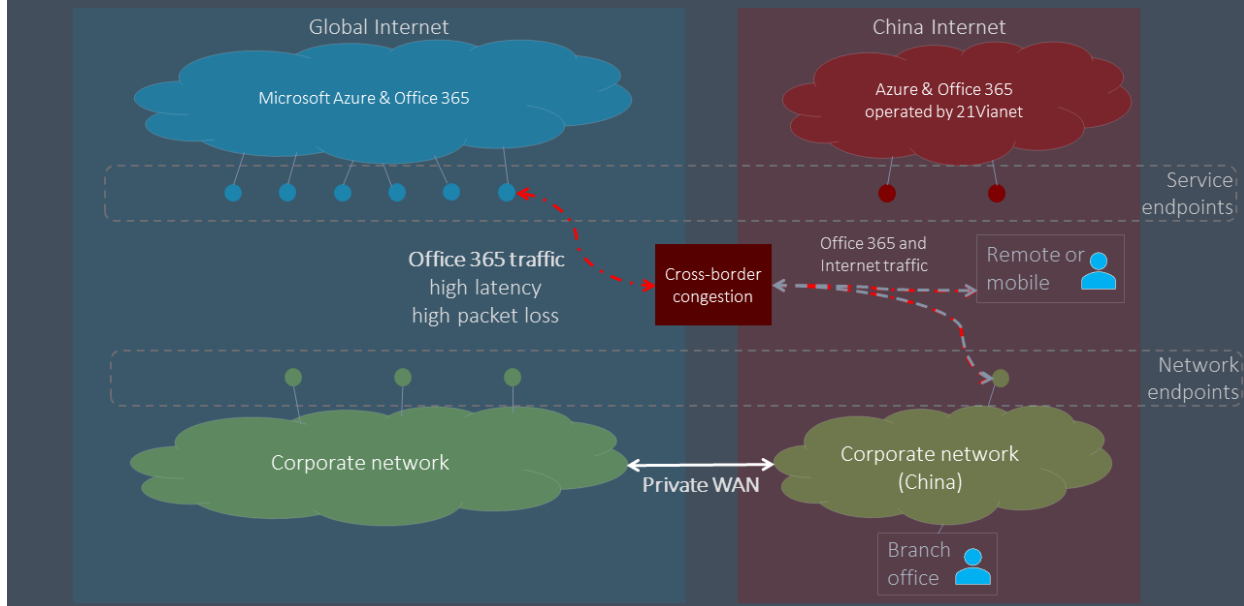
This article is part of a set of articles that address Microsoft 365 optimization for remote users.

- For an overview of using VPN split tunneling to optimize Microsoft 365 connectivity for remote users, see [Overview: VPN split tunneling for Microsoft 365](#).
- For detailed guidance on implementing VPN split tunneling, see [Implementing VPN split tunneling for Microsoft 365](#).
- For a detailed list of VPN split tunneling scenarios, see [Common VPN split tunneling scenarios for Microsoft 365](#).
- For guidance on securing Teams media traffic in VPN split tunneling environments, see [Securing Teams media traffic for VPN split tunneling](#).
- For information about how to configure Stream and live events in VPN environments, see [Special considerations for Stream and live events in VPN environments](#).

For enterprises with global Microsoft 365 tenants and a corporate presence in China, Microsoft 365 client performance for China-based users can be complicated by factors unique to China Telco's Internet architecture.

China ISPs have regulated offshore connections to the global public Internet that go through perimeter devices that are prone to high-levels of cross-border network congestion. This congestion creates packet loss and latency for all Internet traffic going into and out of China.

Global Office 365 access from China, unoptimized



Packet loss and latency are detrimental to the performance of network services, especially services that require large data exchanges (such as large file transfers) or requiring near real-time performance (audio and video applications).

The goal of this topic is to provide best practices for mitigating the impact of China cross-border network congestion on Microsoft 365 services. This topic does not address other common last-mile performance issues such as issues of high packet latency due to complex routing within China carriers.

Corporate network best practices

Many enterprises with global Microsoft 365 tenants and users in China have implemented private networks that carry corporate network traffic between China office locations and offshore locations around the world. These enterprises can leverage this network infrastructure to avoid cross-border network congestion and optimize their Microsoft 365 service performance in China.

IMPORTANT

As with all private WAN implementations, you should always consult regulatory requirements for your country and/or region to ensure that your network configuration is in compliance.

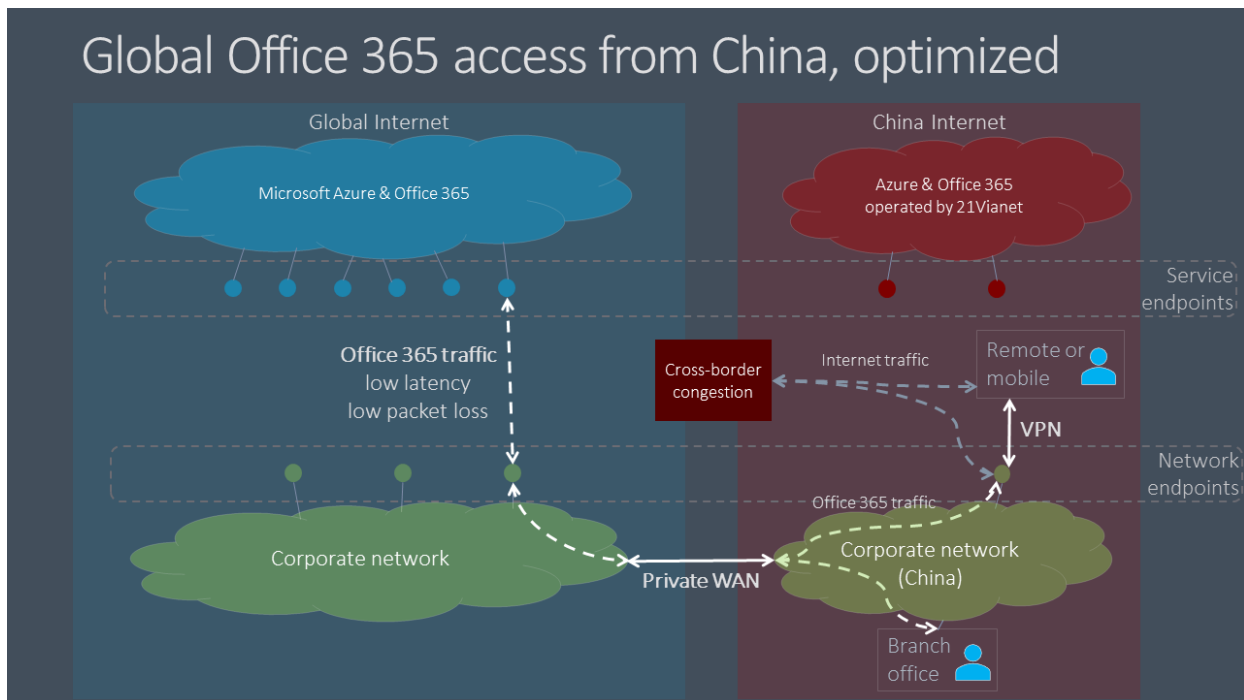
As a first step, it is crucial that you follow our benchmark network guidance at [Network planning and performance tuning for Microsoft 365](#). The primary goal should be to avoid accessing global Microsoft 365 services from the Internet in China if possible.

- Leverage your existing private network to carry Microsoft 365 network traffic between China office networks and offshore locations that egress on the public Internet outside China. Almost any location outside China will provide a clear benefit. Network administrators can further optimize by egressing in areas with low-latency interconnect with the [Microsoft global network](#). Hong Kong, Singapore, Japan, and South Korea are examples.
- Configure user devices to access the corporate network over a VPN connection to allow Microsoft 365 traffic to transit the corporate network's private offshore link. Ensure that VPN clients are either not configured to use split tunneling, or that user devices are configured to ignore split tunneling for Microsoft 365 traffic. For additional information on optimizing VPN connectivity for Teams and real-time media traffic, see [this section](#).
- Configure your network to route all Microsoft 365 traffic across your private offshore link. If you must

minimize the volume of traffic on your private link, you can choose to only route endpoints in the **Optimize** category, and allow requests to **Allow** and **Default** endpoints to transit the Internet. This will improve performance and minimize bandwidth consumption by limiting optimized traffic to critical services that are most sensitive to high latency and packet loss.

- If possible, use UDP instead of TCP for live media streaming traffic, such as for Teams. UDP offers better live media streaming performance than TCP.

For information about how to selectively route Microsoft 365 traffic, see [Managing Office 365 endpoints](#). For a list of all worldwide Office 365 URLs and IP addresses, see [Office 365 URLs and IP address ranges](#).



User best practices

Users in China who connect to global Microsoft 365 tenants from remote locations such as homes, coffee shops, hotels, and branch offices with no connection to enterprise networks can experience poor network performance because traffic between their devices and Microsoft 365 must transit China's congested cross-border network circuits.

If cross-border private networks and/or VPN access into the corporate network are not an option, per-user performance issues can still be mitigated by training your China-based users to follow these best practices.

- Utilize rich Office clients that support caching (e.g. Outlook, Teams, OneDrive, etc.), and avoid web-based clients. Office client caching and offline access features can dramatically reduce the impact of network congestion and latency.
- If your Microsoft 365 tenant has been configured with the *Audio Conferencing* feature, Teams users can join meetings via the public switched telephone network (PSTN). For more information, see [Audio Conferencing in Office 365](#).
- If users experience network performance issues, they should report to their IT department for troubleshooting, and escalate to Microsoft support if trouble with Microsoft 365 services is suspected. Not all issues are caused by cross-border network performance.

Optimizing Microsoft Teams meetings network performance for users in China

For organizations with global Microsoft 365 tenants and a presence in China, Microsoft 365 client performance for China-based users can be complicated by factors unique to the China Internet architecture. Many companies

and schools have reported good results by following this guidance. However, the scope is limited to user network locations that are under control of the IT networking setup, for example, office locations or home/mobile endpoints with VPN connectivity. Microsoft Teams calls and meetings are often used from external locations, such as home offices, mobile locations, on the road, and coffee shops. Because calls and meetings rely on real-time media traffic, these Teams experiences are particularly sensitive to network congestion.

As a result, Microsoft has partnered with telecommunications providers to carry Teams and Skype for Business Online real-time media traffic using a higher-quality, preferential network path between domestic and public internet connections in China and the Teams and Skype services in the Microsoft 365 global cloud. This capability has resulted in a more than ten-fold improvement in packet loss and other key metrics impacting your user's experience.

IMPORTANT

Currently, these improvements do not address attending Microsoft Live Events meetings such as large broadcast or “town hall” style meetings using Teams or Microsoft Stream. The network improvements will benefit users who are presenting or producing a Live Events meeting, because that experience acts as a regular Teams meeting for the producer or presenter.

Organization network best practices for Teams meetings

You need to consider how to leverage these network improvements, given that the previous guidance to consider a private network extension to avoid cross-border network congestion. There are two general options for organization office networks:

1. Do nothing new. Continue to follow the earlier guidance around private network bypass to avoid cross-border congestion. Teams real-time media traffic will leverage that setup, as before.
2. Implement a split/hybrid pattern.
 - Use the previous guidance for all traffic flagged for optimization except Teams meetings and calling real-time media traffic.
 - Route Teams meeting and calling real-time media traffic over the public internet. See the following information for specifics on identifying the real-time media network traffic.

Sending Teams real-time media audio and video traffic over the public internet, which uses the higher quality connectivity, can result in considerable cost savings, because it is free versus paying to send that traffic over a private network. There may be similar additional benefits if users are also using SDWAN or VPN clients. Some organizations may also prefer to have more of their data traverse public internet connections as a general practice.

The same options could apply to SDWAN or VPN configurations. For example, a user is using an SDWAN or VPN to route Microsoft 365 traffic to the corporate network and then leveraging the private extension of that network to avoid cross-border congestion. The user's SDWAN or VPN can now be configured to exclude Teams meeting and calling real-time traffic from the VPN routing. This VPN configuration is referred to as split tunneling. See [VPN split tunneling for Office 365](#) for more information.

You can also continue to use your SDWAN or VPN for all Microsoft 365 traffic, including for Microsoft Teams real-time traffic. Microsoft has no recommendations on the use of SDWAN or VPN solutions.

Home, mobile, and user network best practices for Teams meetings

Users in China can take advantage of these improvements simply by connecting to the public internet service in China with a landline or mobile connection. Teams real-time media audio and video traffic on the public internet directly benefits from improved connectivity and quality.

However, data from other Microsoft 365 services—and other traffic in Teams, such as chat or files—will not directly benefit from these improvements. Users outside the organization network may still experience poor network performance for this traffic. As discussed in this article, you can mitigate these effects by using a VPN

or SDWAN. You can also have your users use rich desktop clients over web clients, which support in-app caching to mitigate network issues.

Identifying Teams real-time media network traffic

For configuring a network device or a VPN/SDWAN setup, you need to exclude only the Teams real-time media audio and video traffic. The traffic details can be found for ID 11 on the official list of [Office 365 URLs and IP address ranges](#). All other network configurations should remain as-is.

Microsoft is continually working to improve the Microsoft 365 user experience and the performance of clients over the widest possible range of network architectures and characteristics. Visit the [Office 365 Networking Tech Community](#) to start or join a conversation, find resources, and submit feature requests and suggestions

Related articles

[Overview: VPN split tunneling for Microsoft 365](#)

[Implementing VPN split tunneling for Microsoft 365](#)

[Common VPN split tunneling scenarios for Microsoft 365](#)

[Securing Teams media traffic for VPN split tunneling](#)

[Special considerations for Stream and live events in VPN environments](#)

[Microsoft 365 Network Connectivity Principles](#)

[Assessing Microsoft 365 network connectivity](#)

[Microsoft 365 network and performance tuning](#)

[Alternative ways for security professionals and IT to achieve modern security controls in today's unique remote work scenarios \(Microsoft Security Team blog\)](#)

[Enhancing VPN performance at Microsoft: using Windows 10 VPN profiles to allow auto-on connections](#)

[Running on VPN: How Microsoft is keeping its remote workforce connected](#)

[Microsoft global network](#)

Azure ExpressRoute for Office 365

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Learn how Azure ExpressRoute is used with Office 365 and how to plan the network implementation project that will be required if you're deploying Azure ExpressRoute for use with Office 365. Infrastructure and platform services running in Azure will often benefit by addressing network architecture and performance considerations. We recommend ExpressRoute for Azure in these cases. Software as a Service offerings like Office 365 and Dynamics 365 have been built to be accessed securely and reliably via the Internet. You can read about Internet performance and security and when you might consider Azure ExpressRoute for Office 365 in the article [Assessing Office 365 network connectivity](#).

NOTE

Microsoft Defender for Endpoint does not provide integration with Azure ExpressRoute. While this does not stop customers from defining ExpressRoute rules that enable connectivity from a private network to Microsoft Defender for Endpoint cloud services, it is up to the customer to maintain rules as the service or cloud infrastructure evolves.

NOTE

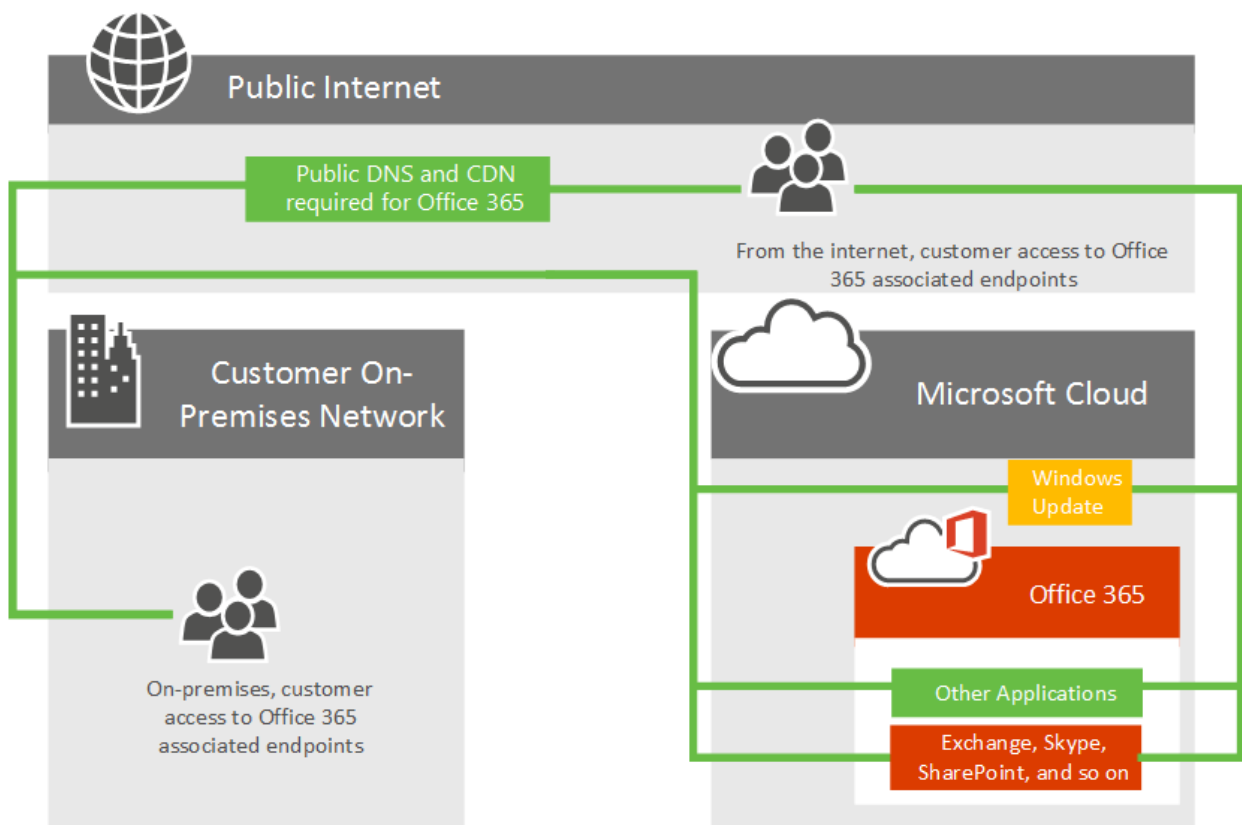
We do not recommend ExpressRoute for Microsoft 365 because it does not provide the best connectivity model for the service in most circumstances. As such, Microsoft authorization is required to use this connectivity model for Microsoft 365. We review every customer request and authorize ExpressRoute for Microsoft 365 only in the rare scenarios where it is necessary. Please read the [ExpressRoute for Microsoft 365 guide](#) for more information and following a comprehensive review of the document with your productivity, network, and security teams, work with your Microsoft account team to submit an exception if needed. Unauthorized subscriptions trying to create route filters for Office 365 will receive an [error message](#).

Planning Azure ExpressRoute for Office 365

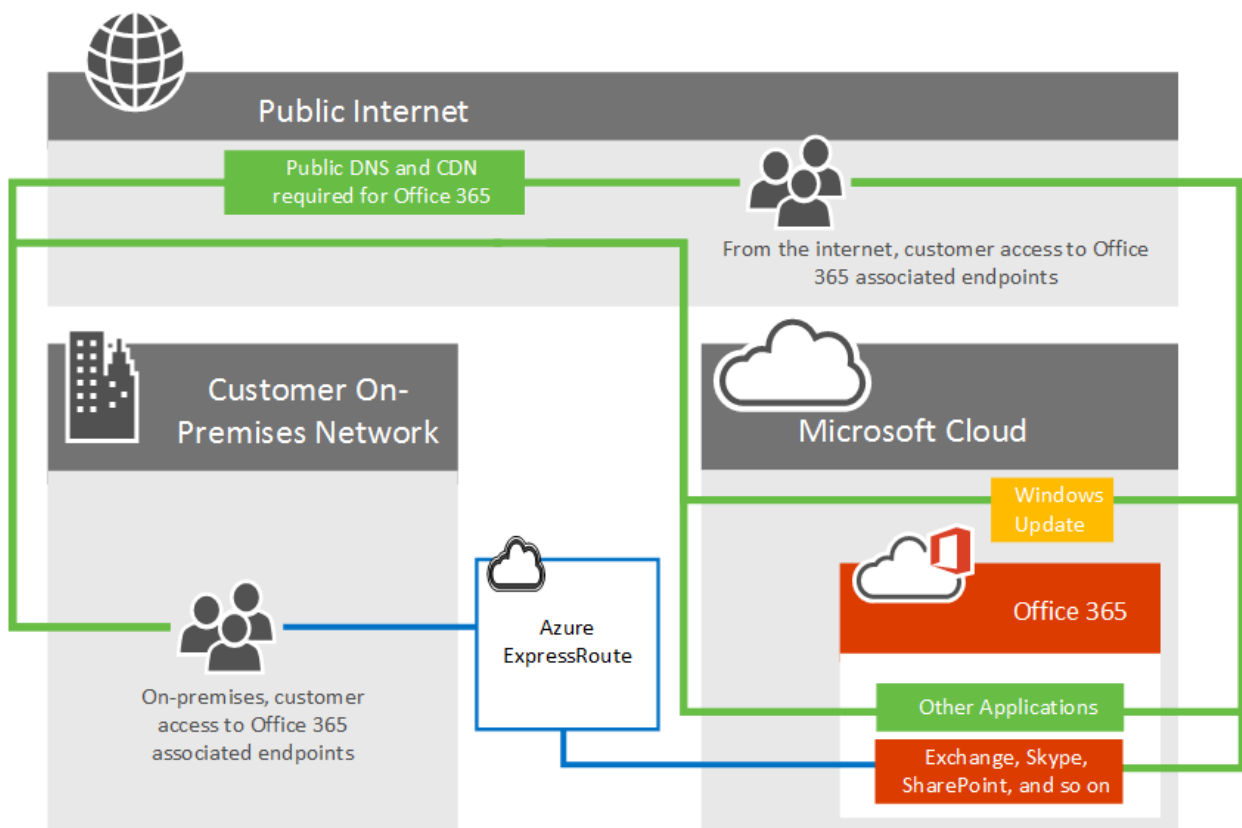
In addition to internet connectivity, you may choose to route a subset of their Office 365 network traffic over a direct connection that offers predictability and a 99.95% uptime SLA for the Microsoft networking components. Azure ExpressRoute provides you with this dedicated network connection to Office 365 and other Microsoft cloud services.

Regardless of whether you have an existing MPLS WAN, ExpressRoute can be added to your network architecture in one of three ways; through a supported cloud exchange co-location provider, an Ethernet point-to-point connection provider, or through an MPLS connection provider. See what [providers are available in your region](#). The direct ExpressRoute connection will enable connectivity to the applications outlined in [What Office 365 services are included?](#) below. Network traffic for all other applications and services will continue to traverse the internet.

Consider the following high level network diagram, which shows a typical Office 365 customer connecting to Microsoft's datacenters over the internet for access to all Microsoft applications such as Office 365, Windows Update, and TechNet. Customers use a similar network path regardless of whether they're connecting from an on-premises network or from an independent internet connection.



Now look at the updated diagram, which depicts an Office 365 customer who uses both the internet and ExpressRoute to connect to Office 365. Notice that some connections such as Public DNS and Content Delivery Network nodes still require the public internet connection. Also notice the customer's users who aren't located in their ExpressRoute connected building are connecting over the Internet.



Still want more information? Learn how to [manage your network traffic with Azure ExpressRoute for Office 365](#) and learn how to [configure Azure ExpressRoute for Office 365](#). We've also recorded a 10 part [Azure ExpressRoute for Office 365 Training](#) series on Channel 9 to help explain the concepts more thoroughly.

What Office 365 services are included?

The following table lists the Office 365 services that are supported over ExpressRoute. Review the [Office 365 endpoints article](#) to understand which network requests for these applications require internet connectivity.

APPLICATIONS INCLUDED
Exchange Online ¹ Exchange Online Protection ¹ Delve ¹
Skype for Business Online ¹ Microsoft Teams ¹
SharePoint Online ¹ OneDrive for Business ¹ Project Online ¹
Portal and shared ¹ Azure Active Directory (Azure AD) ¹ Azure AD Connect ¹ Office ¹

¹ Each of these applications has internet connectivity requirements not supported over ExpressRoute, see the [Office 365 endpoints article](#) for more information.

The services that aren't included with ExpressRoute for Office 365 are Microsoft 365 Apps for enterprise client downloads, On-premises Identity Provider Sign-In, and Office 365 (operated by 21 Vianet) service in China.

Implementing ExpressRoute for Office 365

Implementing ExpressRoute requires the involvement of network and application owners and requires careful planning to determine the new [network routing architecture](#), bandwidth requirements, where security will be implemented, high availability, and so on. To implement ExpressRoute, you'll need to:

1. Fully understand the need ExpressRoute satisfies in your Office 365 connectivity planning. Understand what applications will use the internet or ExpressRoute and fully plan your network capacity, security, and high availability needs in the context of using both the internet and ExpressRoute for Office 365 traffic.
2. Determine the egress and peering locations for both internet and ExpressRoute traffic¹.
3. Determine the capacity required on the internet and ExpressRoute connections.
4. Have a plan in place for implementing security and other standard perimeter controls¹.
5. Have a valid Microsoft Azure account to subscribe to ExpressRoute.
6. Select a connectivity model and an [approved provider](#). Keep in mind, customers can select multiple connectivity models or partners and the partner doesn't need to be the same as your existing network provider.
7. Validate deployment prior to directing traffic to ExpressRoute.
8. Optionally [implement QoS](#) and evaluate regional expansion.

¹ Important performance considerations. Decisions here can dramatically impact latency, which is a critical for applications such as Skype for Business.

For additional references, use our [routing guide](#) in addition to the [ExpressRoute documentation](#).

To purchase ExpressRoute for Office 365, you'll need to work with one or more [approved providers](#) to provision the desired number and size circuits with an ExpressRoute Premium subscription. There are no additional licenses to purchase from Office 365.

Here's a short link you can use to come back: <https://aka.ms/expressrouteoffice365>

Ready to sign up for [ExpressRoute for Office 365](#)?

Related Topics

[Assessing Office 365 network connectivity](#)

[Managing ExpressRoute for Office 365 connectivity](#)

[Routing with ExpressRoute for Office 365](#)

[Network planning with ExpressRoute for Office 365](#)

[Implementing ExpressRoute for Office 365](#)

[Using BGP communities in ExpressRoute for Office 365 scenarios](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 network and performance tuning](#)

See also

[Microsoft 365 Enterprise overview](#)

Implementing ExpressRoute for Office 365

10/28/2022 • 33 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

ExpressRoute for Office 365 provides an alternate routing path to many internet facing Office 365 services. The architecture of ExpressRoute for Office 365 is based on advertising public IP prefixes of Office 365 services that are already accessible over the Internet into your provisioned ExpressRoute circuits for subsequent redistribution of those IP prefixes into your network. With ExpressRoute you effectively enable several different routing paths, through the internet and through ExpressRoute, for many Office 365 services. This state of routing on your network may represent a significant change to how your internal network topology is designed.

Status: Complete Guide v2

You have to carefully plan your ExpressRoute for Office 365 implementation to accommodate for the network complexities of having routing available via both a dedicated circuit with routes injected into your core network and the internet. If you and your team don't perform the detailed planning and testing in this guide, there is a high risk you'll experience intermittent or a total loss of connectivity to Office 365 services when the ExpressRoute circuit is enabled.

To have a successful implementation, you will need to analyze your infrastructure requirements, go through detailed network assessment and design, carefully plan the rollout in a staged and controlled manner, and build a detailed validation and testing plan. For a large, distributed environment it's not uncommon to see implementations span several months. This guide is designed to help you plan ahead.

Large successful deployments may take six months in planning and often include team members from many areas in the organization including networking, Firewall and Proxy server administrators, Office 365 administrators, security, end-user support, project management, and executive sponsorship. Your investment in the planning process will reduce the likelihood that you'll experience deployment failures resulting in downtime or complex and expensive troubleshooting.

We expect the following pre-requisites to be completed before this implementation guide is started.

1. You've completed a network assessment to determine if ExpressRoute is recommended and approved.
2. You've selected an ExpressRoute network service provider. Find details about the [ExpressRoute partners and peering locations](#).
3. You've already read and understand the [ExpressRoute documentation](#) and your internal network is able to meet ExpressRoute pre-requisites end to end.
4. Your team has read all of the public guidance and documentation at <https://aka.ms/expressrouteoffice365>, <https://aka.ms/ert>, and watched the [Azure ExpressRoute for Office 365 Training](#) series on Channel 9 to gain an understanding of critical technical details including:
 - The internet dependencies of SaaS services.
 - How to avoid asymmetric routes and handle complex routing.
 - How to incorporate perimeter security, availability, and application level controls.

Begin by gathering requirements

Start by determining which features and services you plan to adopt within your organization. You need to

determine which features of the different Office 365 services will be used and which locations on your network will host people using those features. With the catalog of scenarios, you need to add the network attributes that each of those scenarios require; such as inbound and outbound network traffic flows and if the Office 365 endpoints are available over ExpressRoute or not.

To gather your organization's requirements:

- Catalog the inbound and outbound network traffic for the Office 365 services your organization is using. Consult Office 365 URLs and IP address ranges page for the description of flows that different Office 365 scenarios require.
- Gather documentation of existing network topology showing details of your internal WAN backbone and topology, connectivity of satellite sites, last mile user connectivity, routing to network perimeter egress points, and proxy services.
 - Identify inbound service endpoints on the network diagrams that Office 365 and other Microsoft services will connect to, showing both internet and proposed ExpressRoute connection paths.
 - Identify all geographic user locations and WAN connectivity between locations along with which locations currently have an egress to the internet and which locations are proposed to have an egress to an ExpressRoute peering location.
 - Identify all edge devices, such as proxies, firewalls, and so on, and catalog their relationship to flows going over the Internet and ExpressRoute.
 - Document whether end users will access Office 365 services via Direct Routing or indirect application proxy for both Internet and ExpressRoute flows.
- Add the location of your tenant and meet-me locations to your network diagram.
- Estimate the expected and observed network performance and latency characteristics from major user locations to Office 365. Keep in mind that Office 365 is a global and distributed set of services and users will be connecting to locations that may be different from the location of their tenant. For this reason, it is recommended to measure and optimize for latency between the user and the closest edge of Microsoft global network over ExpressRoute and Internet connections. You can use your findings from the network assessment to aid with this task.
- List company network security and high availability requirements that need to be met with the new ExpressRoute connection. For example, how do users continue to get access to Office 365 in the event of the Internet egress or ExpressRoute circuit failure.
- Document which inbound and outbound Office 365 network flows will use the Internet path and which will use ExpressRoute. The specifics of geographical locations of your users and details of your on-premises network topology may require the plan to be different from one user location to another.

Catalog your outbound and inbound network traffic

To minimize routing and other network complexities, we recommend that you only use ExpressRoute for Office 365 for the network traffic flows that are required to go over a dedicated connection due to regulatory requirements or as the result of the network assessment. Additionally, we recommend that you stage the scope of ExpressRoute routing and approach outbound and inbound network traffic flows as different and distinct stages of the implementation project. Deploy ExpressRoute for Office 365 for just user initiated outbound network traffic flows and leave inbound network traffic flows across the Internet can help to control the increase in topological complexity and risks of introducing additional asymmetric routing possibilities.

Your network traffic catalog should contain listings of all the inbound and outbound network connections that you'll have between your on-premises network and Microsoft.

- Outbound network traffic flows are any scenarios where a connection is initiated from your on-premises environment, such as from internal clients or servers, with a destination of the Microsoft services. These connections may be direct to Office 365 or indirect, such as when the connection goes through proxy servers, firewalls, or other networking devices on the path to Office 365.
- Inbound network traffic flows are any scenarios where a connection is initiated from the Microsoft cloud to an on-premises host. These connections typically need to go through firewall and other security infrastructure that customer security policy requires for externally originated flows.

Read the **Ensuring route symmetry** section of the article [Routing with ExpressRoute for Office 365](#) to determine which services will send inbound traffic and look for the column marked **ExpressRoute for Office 365** in the [Office 365 endpoints](#) reference article to determine the rest of the connectivity information.

For each service that requires an outbound connection, you'll want to describe the planned connectivity for the service including network routing, proxy configuration, packet inspection, and bandwidth needs.

For each service that requires an inbound connection, you'll need some additional information. Servers in the Microsoft cloud will establish connections to your on-premises network. To ensure the connections are made correctly, you'll want to describe all aspects of this connectivity, including; the public DNS entries for the services that will accept these inbound connections, the CIDR formatted IPv4 IP addresses, which ISP equipment is involved, and how inbound NAT or source NAT is handled for these connections.

Inbound connections should be reviewed regardless of whether they're connecting over the internet or ExpressRoute to ensure asymmetric routing hasn't been introduced. In some cases, on-premises endpoints that Office 365 services initiate inbound connections to may also need to be accessed by other Microsoft and non-Microsoft services. It is paramount that enabling ExpressRoute routing to these services for Office 365 purposes doesn't break other scenarios. In many cases, customers may need to implement specific changes to their internal network, such as source-based NAT, to ensure that inbound flows from Microsoft remain symmetric after ExpressRoute is enabled.

Here's a sample of the level of detail required. In this case Exchange Hybrid would route to the on-premises system over ExpressRoute.

CONNECTION PROPERTY	VALUE
Network traffic direction	Inbound
Service	Exchange Hybrid
Public Office 365 endpoint (source)	Exchange Online (IP addresses)
Public On-Premises Endpoint (destination)	5.5.5.5
Public (Internet) DNS entry	Autodiscover.contoso.com
Will this on-premises endpoint be used for by other (non-Office 365) Microsoft services	No
Will this on-premises endpoint be used by users/systems on the Internet	Yes
Internal systems published through public endpoints	Exchange Server client access role (on-premises) 192.168.101, 192.168.102, 192.168.103
IP advertisement of the public endpoint	To Internet: 5.5.0.0/16 To ExpressRoute: 5.5.5.0/24

CONNECTION PROPERTY	VALUE
Security/Perimeter Controls	Internet path: DeviceID_002 ExpressRoute path: DeviceID_003
High Availability	Active/Active across 2 geo-redundant / ExpressRoute circuits - Chicago and Dallas
Path symmetry control	Method: Source NAT Internet path: Source NAT inbound connections to 192.168.5.5 ExpressRoute path: Source NAT connections to 192.168.1.0 (Chicago) and 192.168.2.0 (Dallas)

Here's a sample of a service that is outbound only:

CONNECTION PROPERTY	VALUE
Network traffic direction	Outbound
Service	SharePoint Online
On-premises endpoint (source)	User workstation
Public Office 365 endpoint (destination)	SharePoint Online (IP addresses)
Public (Internet) DNS entry	*.sharepoint.com (and more FQDNs)
CDN Referrals	cdn.sharepointonline.com (and more FQDNs) - IP addresses maintained by CDN providers
IP advertisement and NAT in use	Internet path/Source NAT: 1.1.1.0/24 ExpressRoute path/Source NAT: 1.1.2.0/24 (Chicago) and 1.1.3.0/24 (Dallas)
Connectivity method	Internet: via layer 7 proxy (.pac file) ExpressRoute: direct routing (no proxy)
Security/Perimeter Controls	Internet path: DeviceID_002 ExpressRoute path: DeviceID_003
High Availability	Internet path: Redundant internet egress ExpressRoute path: Active/Active 'hot potato' routing across 2 geo-redundant ExpressRoute circuits - Chicago and Dallas
Path symmetry control	Method: Source NAT for all connections

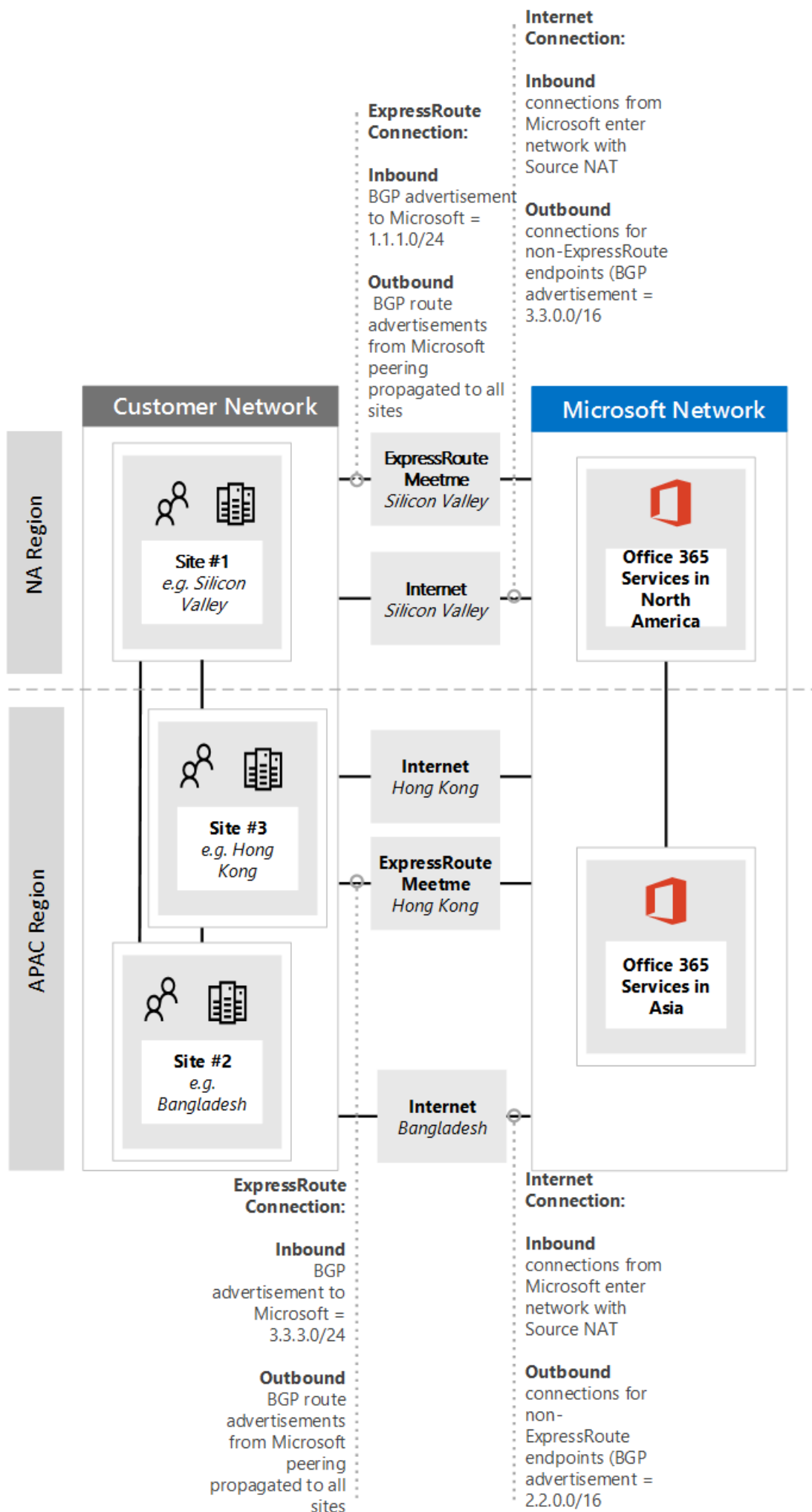
Your network topology design with regional connectivity

Once you understand the services and their associated network traffic flows, you can create a network diagram that incorporates these new connectivity requirements and illustrates the changes you'll make to use ExpressRoute for Office 365. Your diagram should include:

1. All user locations where Office 365 and other services will be accessed from.
2. All internet and ExpressRoute egress points.

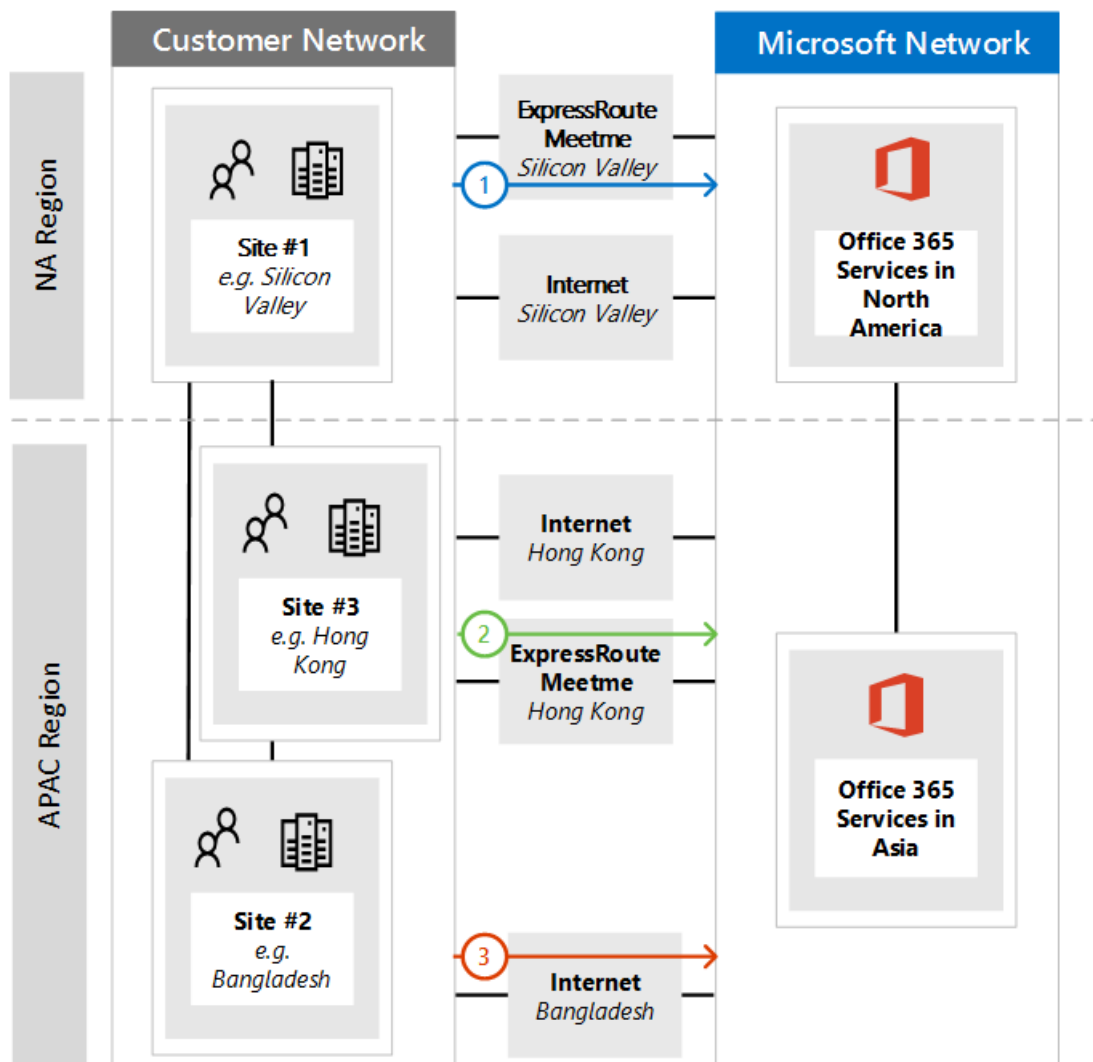
3. All outbound and inbound devices that manage connectivity in and out of the network, including routers, firewalls, application proxy servers, and intrusion detection/prevention.
4. Internal destinations for all inbound traffic, such as internal ADFS servers that accept connections from the ADFS web application proxy servers.
5. Catalog of all IP subnets that will be advertised
6. Identify each location where people will access Office 365 from and list the meet-me locations that will be used for ExpressRoute.
7. Locations and portions of your internal network topology, where Microsoft IP prefixes learned from ExpressRoute will be accepted, filtered, and propagated to.
8. The network topology should illustrate the geographic location of each network segment and how it connects to the Microsoft network over ExpressRoute and/or the Internet.

The diagram below shows each location where people will be using Office 365 from along with the inbound and outbound routing advertisements to Office 365.



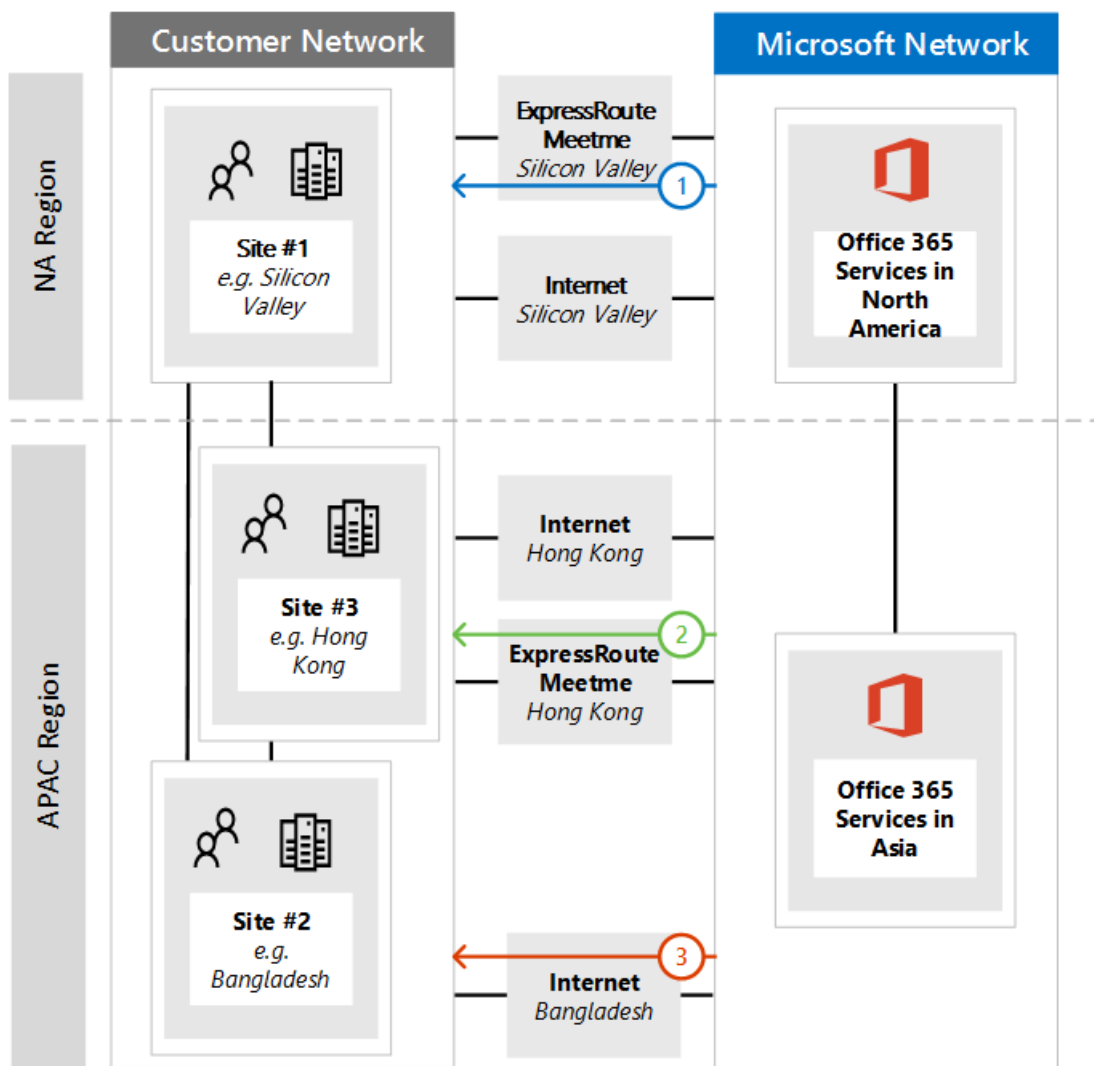
For outbound traffic, the people access Office 365 in one of three ways:

1. Through a meet-me location in North America for the people in California.
2. Through a meet-me location in Hong Kong for the people in Hong Kong.
3. Through the internet in Bangladesh where there are fewer people and no ExpressRoute circuit provisioned.



Similarly, the inbound network traffic from Office 365 returns in one of three ways:

1. Through a meet-me location in North America for the people in California.
2. Through a meet-me location in Hong Kong for the people in Hong Kong.
3. Through the internet in Bangladesh where there are fewer people and no ExpressRoute circuit provisioned.



Determine the appropriate meet-me location

The selection of meet-me locations, which are the physical location where your ExpressRoute circuit connects your network to the Microsoft network, is influenced by the locations where people will access Office 365 from. As a SaaS offering, Office 365 does not operate under the IaaS or PaaS regional model in the same way Azure does. Instead, Office 365 is a distributed set of collaboration services, where users may need to connect to endpoints across multiple datacenters and regions, which may not necessarily be in the same location or region where the user's tenant is hosted.

This means the most important consideration you need to make when selecting meet-me locations for ExpressRoute for Office 365 is where the people in your organization will be connecting from. The general recommendation for optimal Office 365 connectivity is implement routing, so that user requests to Office 365 services are handed off into the Microsoft network over the shortest network path, this is also often being referred to as 'hot potato' routing. For example, if most of the Office 365 users are in one or two locations, selecting meet-me locations that are in the closest proximity to the location of those users will create the optimal design. If your company has large user populations in many different regions, you may want to consider having multiple ExpressRoute circuits and meet-me locations. For some of your user locations, the shortest/most optimal path into Microsoft network and Office 365, may not be through your internal WAN and ExpressRoute meet-me points, but via the Internet.

Often, there are multiple meet-me locations that could be selected within a region with relative proximity to your users. Fill out the following table to guide your decisions.

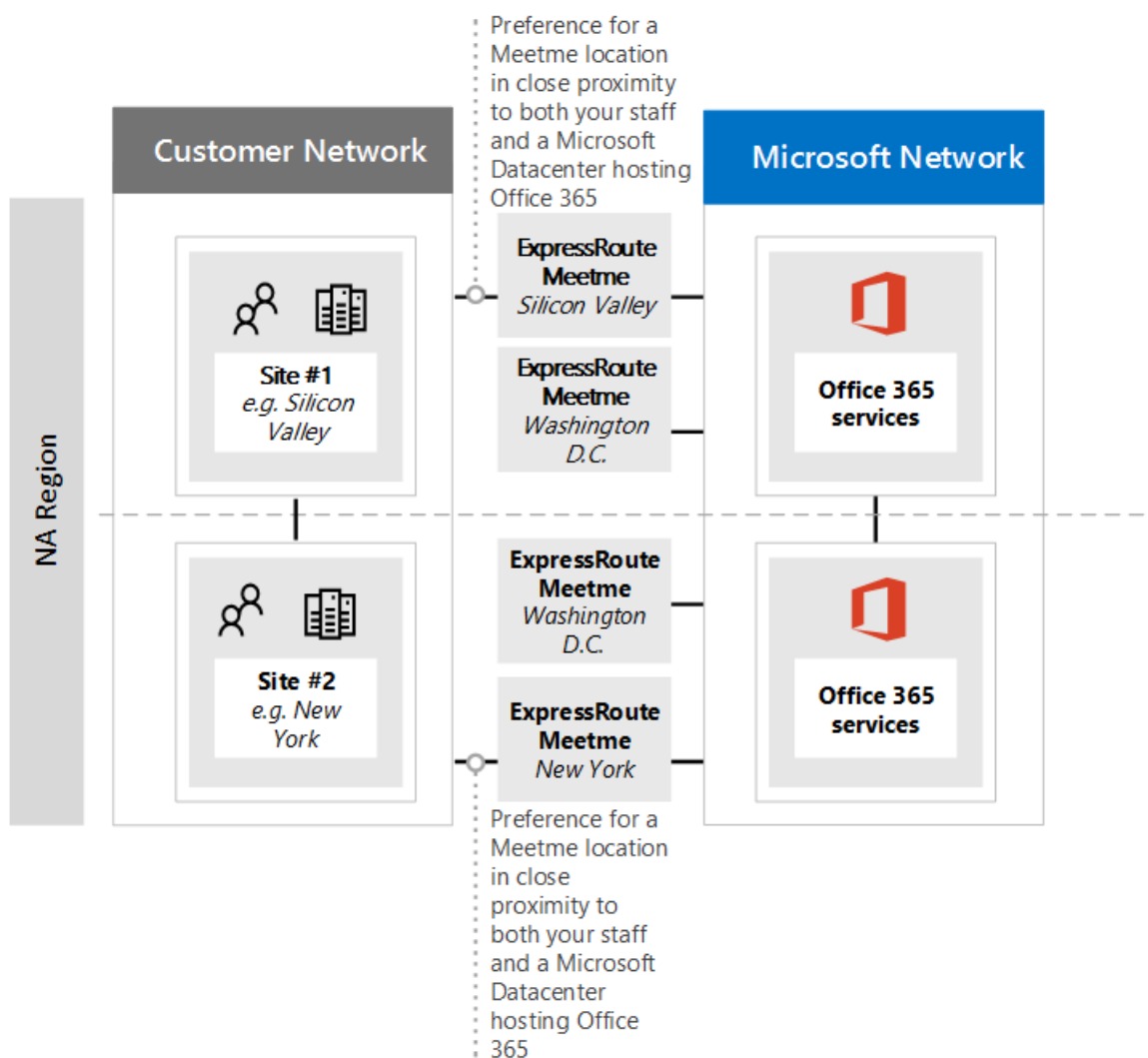
Planned ExpressRoute meet-me locations in California and New York

LOCATION	NUMBER OF PEOPLE	EXPECTED LATENCY TO MICROSOFT NETWORK OVER INTERNET EGRESS	EXPECTED LATENCY TO MICROSOFT NETWORK OVER EXPRESSROUTE
Los Angeles	10,000	~15ms	~10ms (via Silicon Valley)
Washington DC	15,000	~20ms	~10ms (via New York)
Dallas	5,000	~15ms	~40ms (via New York)

Once the global network architecture showing the Office 365 region, ExpressRoute network service provider meet-me locations, and the quantity of people by location has been developed, it can be used to identify if any optimizations can be made. It may also show global hairpin network connections where traffic routes to a distant location in order to get the meet-me location. If a hairpin on the global network is discovered, it should be remediated before continuing. Either find another meet-me location, or use selective Internet breakout egress points to avoid the hairpin.

The first diagram, shows an example of a customer with two physical locations in North America. You can see the information about office locations, Office 365 tenant locations, and several choices for ExpressRoute meet-me locations. In this example, the customer has selected the meet-me location based on two principles, in order:

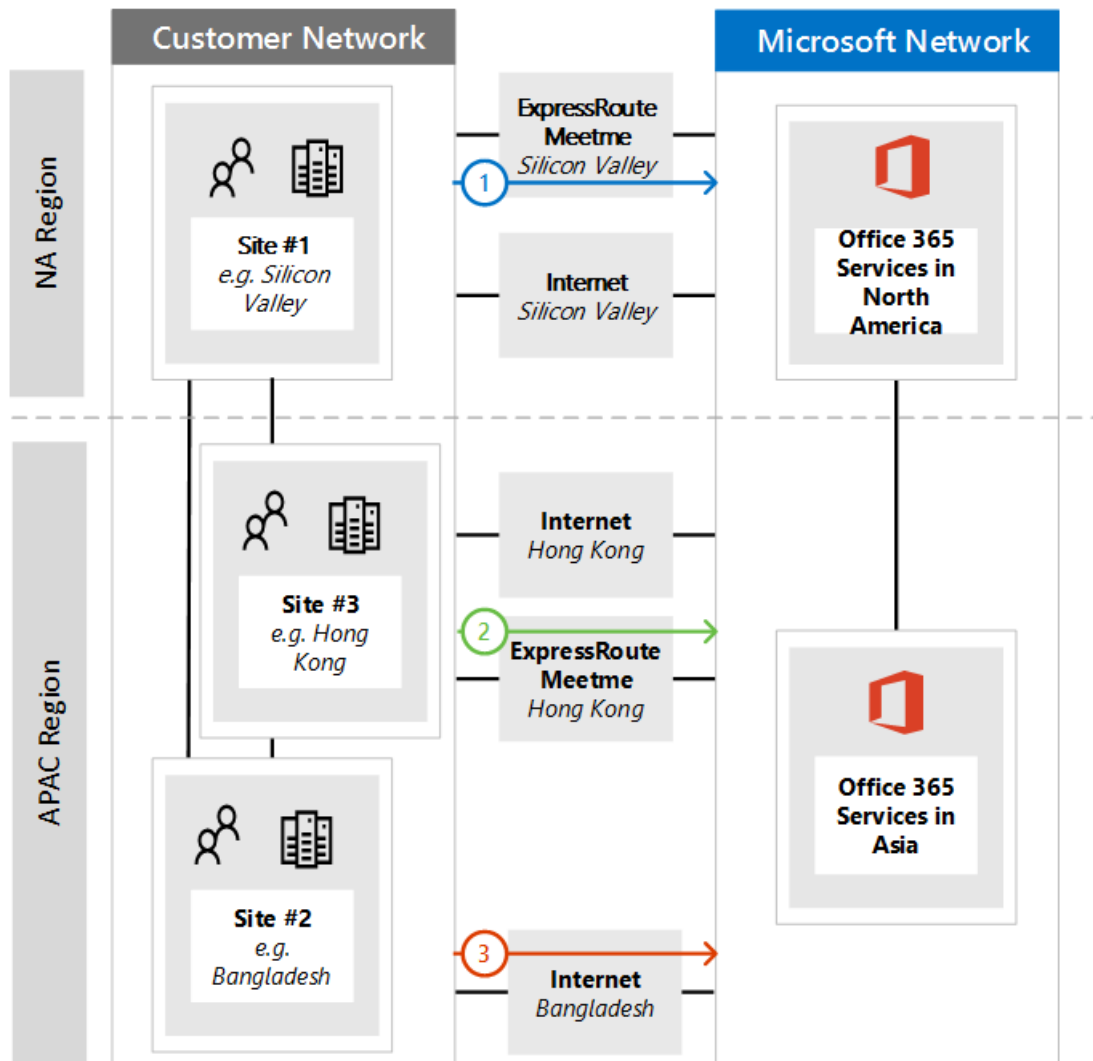
1. Closest proximity to the people in their organization.
2. Closest in proximity to a Microsoft datacenter where Office 365 is hosted.



Expanding this concept slightly further, the second diagram shows an example multi-national customer faced

with similar information and decision making. This customer has a small office in Bangladesh with only a small team of ten people focused on growing their footprint in the region. There is a meet-me location in Chennai and a Microsoft datacenter with Office 365 hosted in Chennai so a meet-me location would make sense; however, for ten people, the expense of the extra circuit is burdensome. As you look at your network, you'll need to determine if the latency involved in sending your network traffic across your network is more effective than spending the capital to acquire another ExpressRoute circuit.

Alternatively, the ten people in Bangladesh may experience better performance with their network traffic sent over the internet to the Microsoft network than they would routing on their internal network as we showed in the introductory diagrams and reproduced below.



Create your ExpressRoute for Office 365 implementation plan

Your implementation plan should encompass both the technical details of configuring ExpressRoute and the details of configuring all the other infrastructure on your network, such as the following.

- Plan which services split between ExpressRoute and Internet.
- Plan for bandwidth, security, high availability, and failover.
- Design inbound and outbound routing, including proper routing path optimizations for different locations
- Decide how far ExpressRoute routes will be advertised into your network and what is the mechanism for clients to select Internet or ExpressRoute path; for example, direct routing or application proxy.
- Plan DNS record changes, including [Sender Policy Framework](#) entries.

- Plan NAT strategy including outbound and inbound source NAT.

Plan your routing with both internet and ExpressRoute network paths

- For your initial deployment, all inbound services, such as inbound email or hybrid connectivity, are recommended to use the internet.
- Plan end-user client LAN routing, such as [configuring a PAC/WPAD file](#), default route, proxy servers, and BGP route advertisements.
- Plan perimeter routing, including proxy servers, firewalls, and cloud proxies.

Plan your bandwidth, security, high availability, and failover

Create a plan for bandwidth required for each major Office 365 workload. Separately estimate Exchange Online, SharePoint Online, and Skype for Business Online bandwidth requirements. You can use the estimation calculators we've provided for Exchange Online and Skype for Business as a starting place; however, a pilot test with a representative sample of the user profiles and locations is required to fully understand the bandwidth needs of your organization.

Add how security is handled at each internet and ExpressRoute egress location to your plan, remember all ExpressRoute connections to Office 365 use public peering and must still be secured in accordance with your company security policies of connecting to external networks.

Add details to your plan about which people will be affected by what type of outage and how those people will be able to perform their work at full capacity in the simplest manner.

Plan bandwidth requirements including Skype for Business requirements on Jitter, Latency, Congestion, and Headroom

Skype for Business Online also has specific extra network requirements, which are detailed in the article [Media Quality and Network Connectivity Performance in Skype for Business Online](#).

Read the section **Bandwidth planning for Azure ExpressRoute** in [Network planning with ExpressRoute for Office 365](#).

When performing a bandwidth assessment with your pilot users, you can use our guide; [Office 365 performance tuning using baselines and performance history](#).

Plan for high availability requirements

Create a plan for high availability to meet your needs and incorporate this into your updated network topology diagram. Read the section **High availability and failover with Azure ExpressRoute** in [Network planning with ExpressRoute for Office 365](#).

Plan for network security requirements

Create a plan to meet your network security requirements and incorporate this into your updated network topology diagram. Read the section **Applying security controls to Azure ExpressRoute for Office 365 scenarios** in [Network planning with ExpressRoute for Office 365](#).

Design outbound service connectivity

ExpressRoute for Office 365 has *outbound* network requirements that may be unfamiliar. Specifically, the IP addresses that represent your users and networks to Office 365 and act as the source endpoints for outbound network connections to Microsoft must follow specific requirements outlined below.

1. The endpoints must be public IP addresses, that are registered to your company or to carrier providing ExpressRoute connectivity to you.
2. The endpoints must be advertised to Microsoft and validated/accepted by ExpressRoute.
3. The endpoints must not be advertised to the Internet with the same or more preferred routing metric.

4. The endpoints must not be used for connectivity to Microsoft services that are not configured over ExpressRoute.

If your network design doesn't meet these requirements, there is a high risk your users will experience connectivity failures to Office 365 and other Microsoft services due to route black holing or asymmetric routing. This occurs when requests to Microsoft services are routed over ExpressRoute, but responses are routed back across the internet, or vice versa, and the responses are dropped by stateful network devices such as firewalls.

The most common method you can use to meet the above requirements is to use source NAT, either implemented as a part of your network or provided by your ExpressRoute carrier. Source NAT allows you to abstract the details and private IP addressing of your internet network from ExpressRoute and; coupled with proper IP route advertisements, provide an easy mechanism to ensure path symmetry. If you're using stateful network devices that are specific to ExpressRoute peering locations, you must implement separate NAT pools for each ExpressRoute peering to ensure path symmetry.

Read more about the [ExpressRoute NAT requirements](#).

Add the changes for the outbound connectivity to the network topology diagram.

Design inbound service connectivity

Most enterprise Office 365 deployments assume some form of inbound connectivity from Office 365 to on-premises services, such as for Exchange, SharePoint, and Skype for Business hybrid scenarios, mailbox migrations, and authentication using ADFS infrastructure. When ExpressRoute you enable an extra routing path between your on-premises network and Microsoft for outbound connectivity, these inbound connections may inadvertently be impacted by asymmetric routing, even if you intend to have those flows continue to use the Internet. A few precautions described below are recommended to ensure there is no impact to Internet based inbound flows from Office 365 to on-premises systems.

To minimize the risks of asymmetric routing for inbound network traffic flows, all of the inbound connections should use source NAT before they're routed into segments of your network, which have routing visibility into ExpressRoute. If the incoming connections are allowed onto a network segment with routing visibility into ExpressRoute without source NAT, requests originating from Office 365 will enter from the internet, but the response going back to Office 365 will prefer the ExpressRoute network path back to the Microsoft network, causing asymmetric routing.

You may consider one of the following implementation patterns to satisfy this requirement:

1. Perform source NAT before requests are routed into your internal network using networking equipment such as firewalls or load balancers on the path from the Internet to your on-premises systems.
2. Ensure that ExpressRoute routes are not propagated to the network segments where inbound services, such as front-end servers or reverse proxy systems, handling Internet connections reside.

Explicitly accounting for these scenarios in your network and keeping all inbound network traffic flows over the Internet helps to minimize deployment and operational risk of asymmetric routing.

There may be cases where you may choose to direct some inbound flows over ExpressRoute connections. For these scenarios, take the following extra considerations into account.

1. Office 365 can only target on-premises endpoints that use public IPs. This means that even if the on-premises inbound endpoint is only exposed to Office 365 over ExpressRoute, it still needs to have public IP associated with it.
2. All DNS name resolution that Office 365 services perform to resolve on-premises endpoints happen using public DNS. This means that you must register inbound service endpoints' FQDN to IP mappings on the Internet.

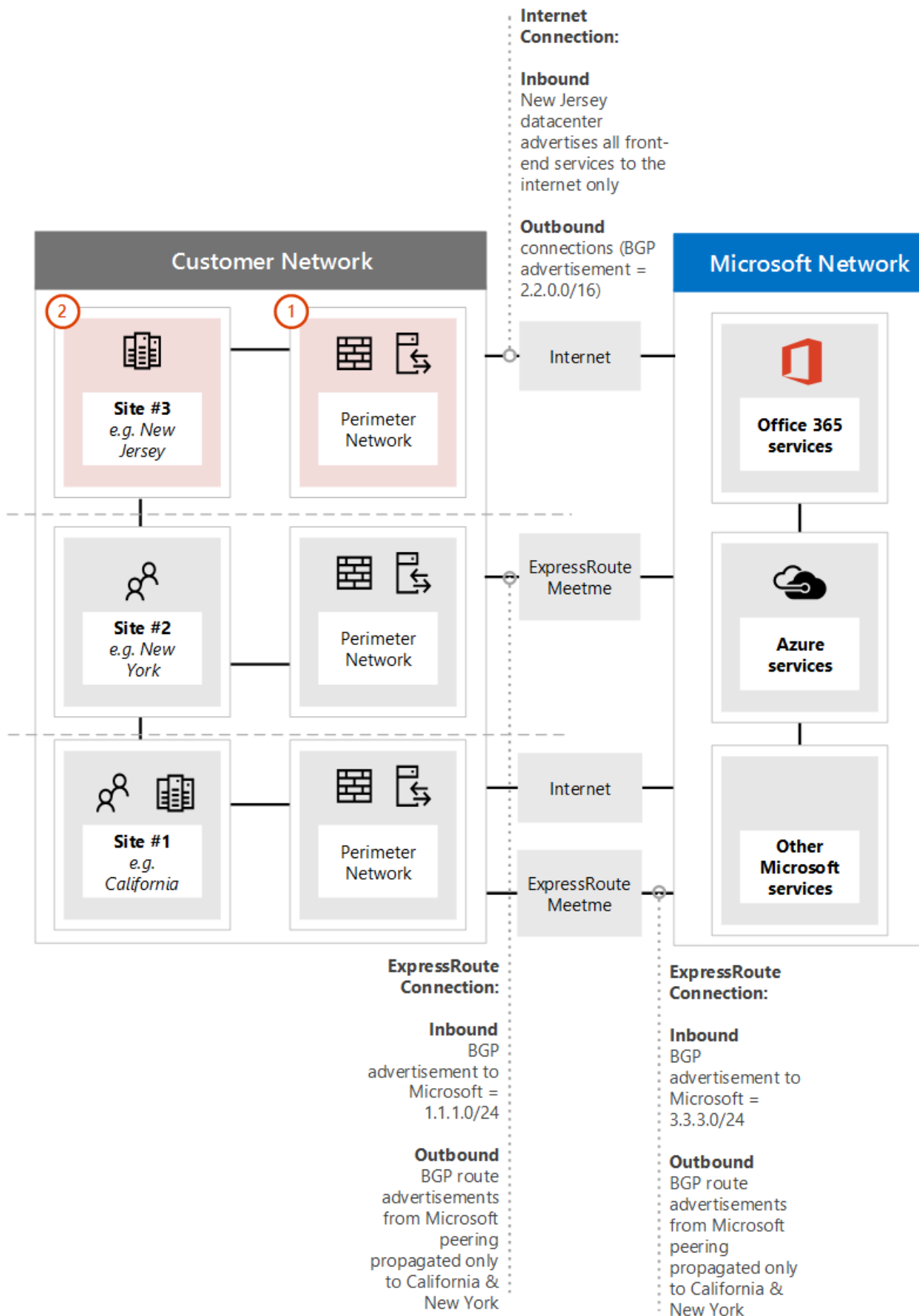
3. In order to receive inbound network connections over ExpressRoute, the public IP subnets for these endpoints must be advertised to Microsoft over ExpressRoute.
4. Carefully evaluate these inbound network traffic flows to ensure that proper security and network controls are applied to them in accordance with your company security and network policies.
5. Once your on-premises inbound endpoints are advertised to Microsoft over ExpressRoute, ExpressRoute will effectively become the preferred routing path to those endpoints for all Microsoft services, including Office 365. This means that those endpoint subnets must only be used for communications with Office 365 services and no other services on the Microsoft network. Otherwise, your design will cause asymmetric routing where inbound connections from other Microsoft services prefer to route inbound over ExpressRoute, while the return path will use the Internet.
6. In the event an ExpressRoute circuit or meet-me location is down, you'll need to ensure the on-premises inbound endpoints are still available to accept requests over a separate network path. This may mean advertising subnets for those endpoints through multiple ExpressRoute circuits.
7. We recommend applying source NAT for all inbound network traffic flows entering your network through ExpressRoute, especially when these flows cross stateful network devices such as firewalls.
8. Some on-premises services, such as ADFS proxy or Exchange autodiscover, may receive inbound requests from both Office 365 services and users from the Internet. For these requests Office 365 will target the same FQDN as user requests over the Internet. Allowing inbound user connections from the internet to those on-premises endpoints, while forcing Office 365 connections to use ExpressRoute, represents significant routing complexity. For the vast majority of customers implementing such complex scenarios over ExpressRoute is not recommended due to operational considerations. This additional overhead includes, managing risks of asymmetric routing and will require you to carefully manage routing advertisements and policies across multiple dimensions.

Update your network topology plan to show how you would avoid asymmetric routes

You want to avoid asymmetric routing to ensure people in your organization can seamlessly use Office 365 as well as other important services on the internet. There are two common configurations customers have that cause asymmetric routing. Now's a good time to review the network configuration you're planning to use and check if one of these asymmetric routing scenarios could exist.

To begin, we'll examine a few different situations associated with the following network diagram. In this diagram, all servers that receive inbound requests, such as ADFS or on-premises hybrid servers are in the New Jersey data center and are advertised to the internet.

1. While the perimeter network is secure, there is no Source NAT available for incoming requests.
2. The servers in the New Jersey data center are able to see both internet and ExpressRoute routes.



We also have suggestions on how to fix them.

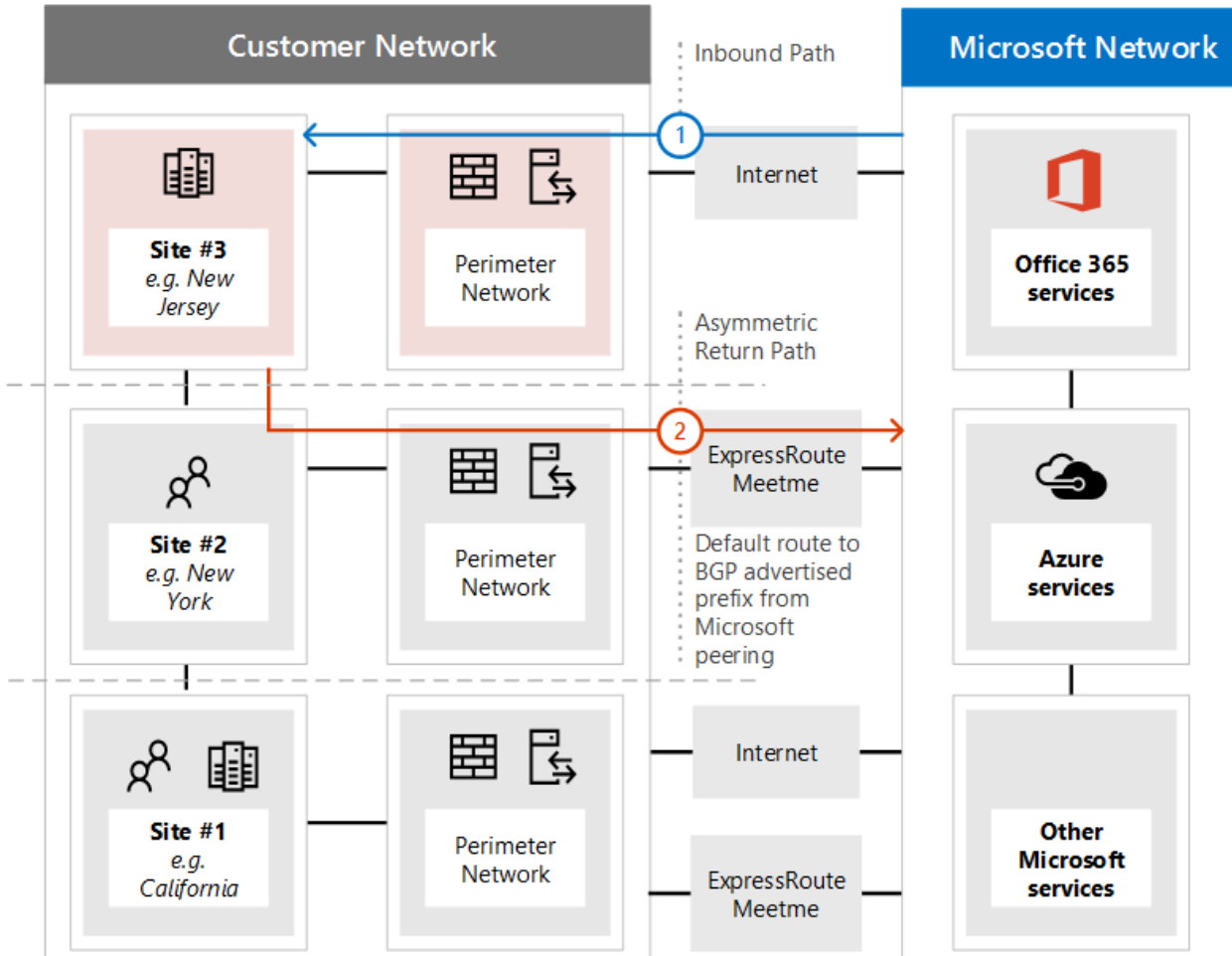
Problem 1: Cloud to on-premises connection over the Internet

The following diagram illustrates the asymmetric network path taken when your network configuration doesn't provide NAT for inbound requests from the Microsoft cloud over the internet.

1. The inbound request from Office 365 retrieves the IP address of the on-premises endpoint from public

DNS and sends the request to your perimeter network.

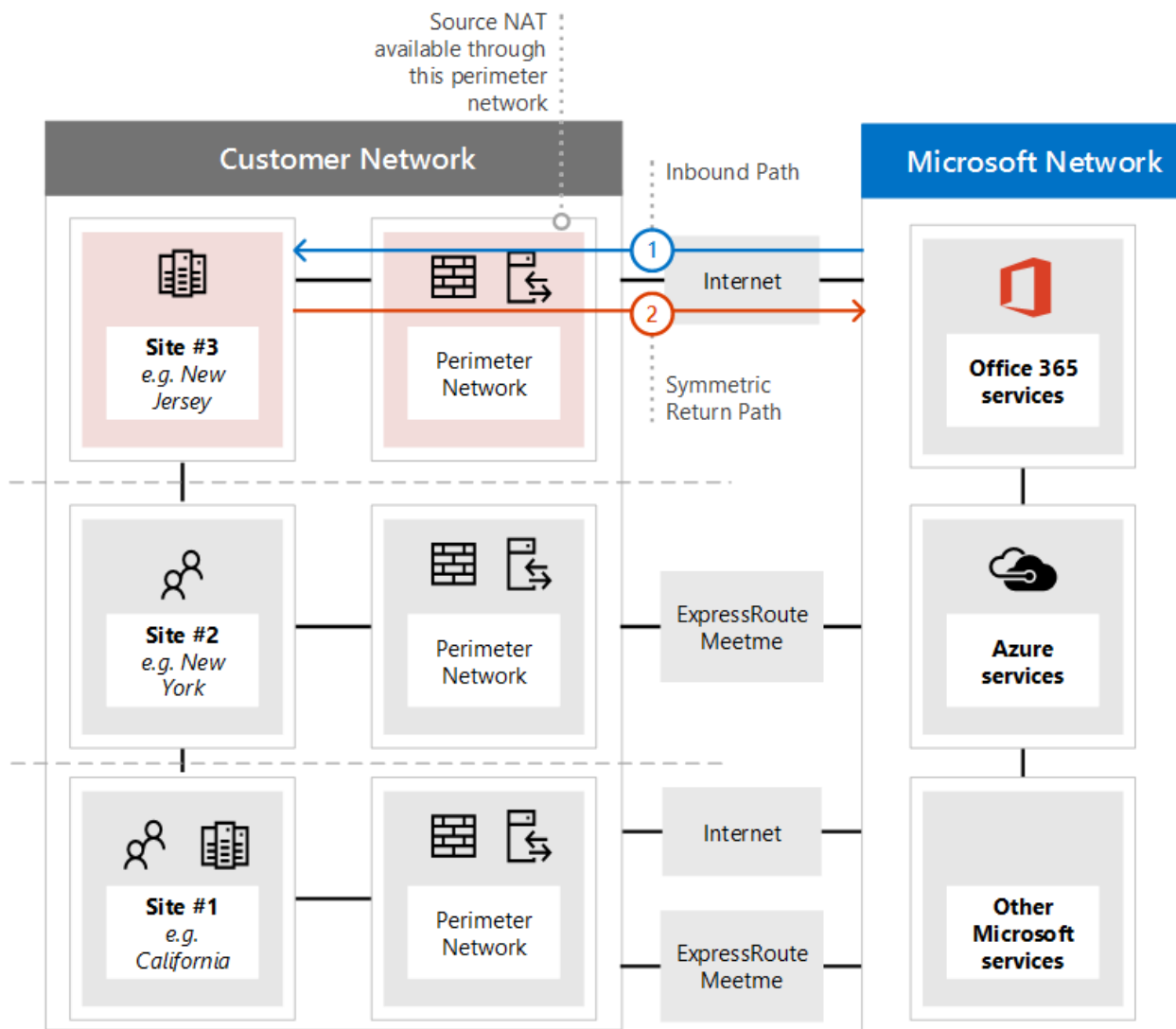
2. In this faulty configuration, there is no Source NAT configured or available at the perimeter network where the traffic is sent resulting in the actual source IP address being used as the return destination.
- The server on your network routes the return traffic to Office 365 through any available ExpressRoute network connection.
 - The result is an Asymmetric path for that flow to Office 365, resulting in a broken connection.



Solution 1a: Source NAT

Simply adding a source NAT to the inbound request resolves this misconfigured network. In this diagram:

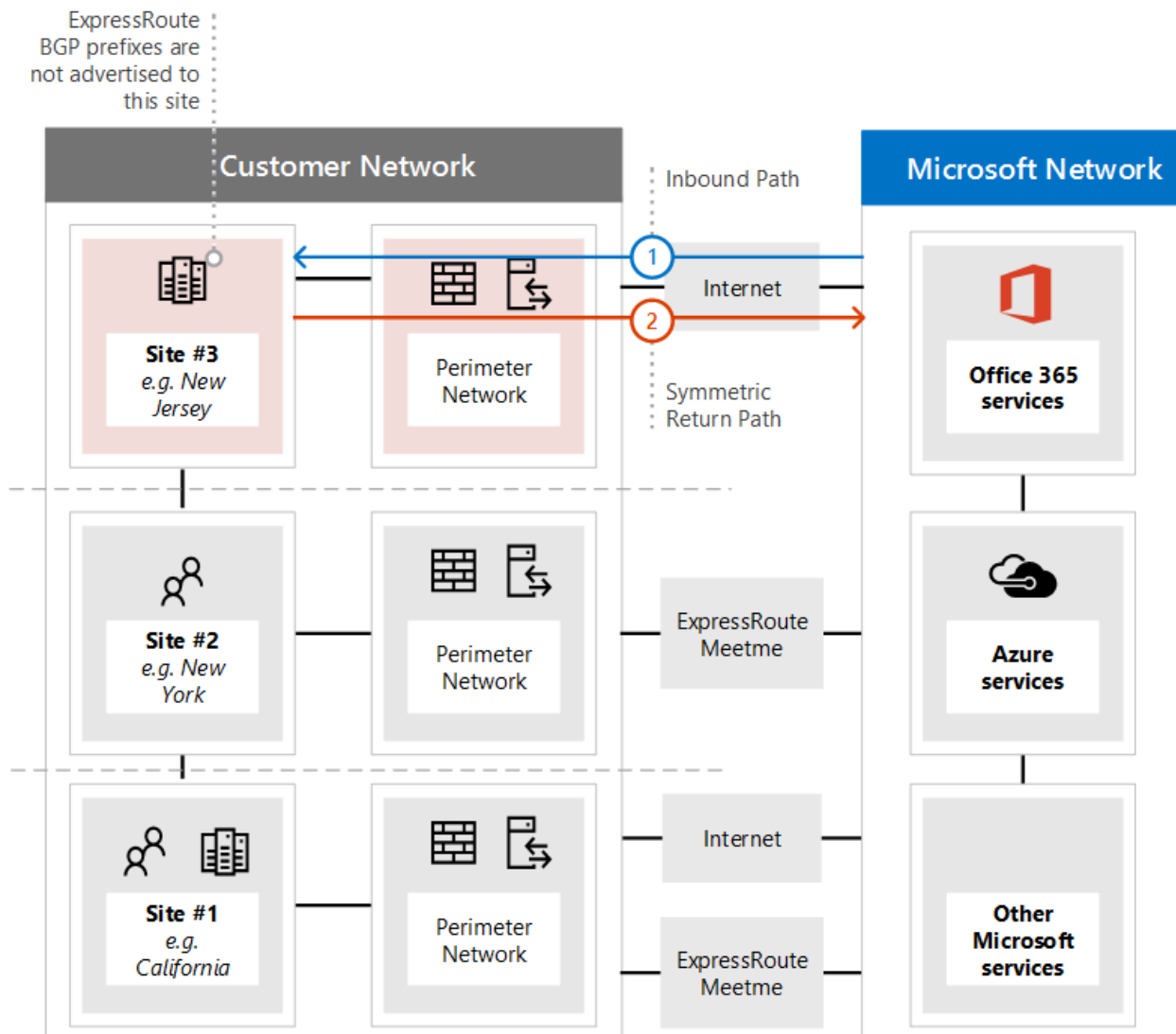
1. The incoming request continues to enter through the New Jersey data center's perimeter network. This time Source NAT is available.
2. The response from the server routes back toward the IP associated with the Source NAT instead of the original IP address, resulting in the response returning along the same network path.



Solution 1b: Route Scoping

Alternatively, you can choose to not allow the ExpressRoute BGP prefixes to be advertised, removing the alternate network path for those computers. In this diagram:

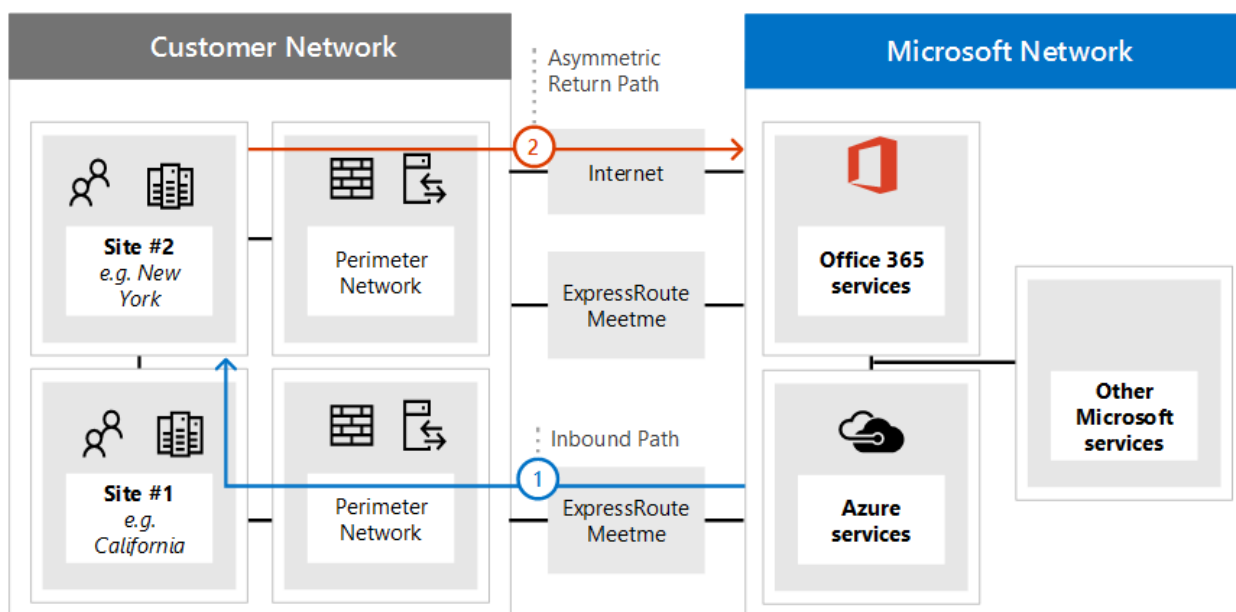
1. The incoming request continues to enter through the New Jersey data center's perimeter network. This time the prefixes advertised from Microsoft over the ExpressRoute circuit are not available to the New Jersey data center.
2. The response from the server routes back toward the IP associated with the original IP address over the only route available, resulting in the response returning along the same network path.



Problem 2: Cloud to on-premises connection over ExpressRoute

The following diagram illustrates the asymmetric network path taken when your network configuration doesn't provide NAT for inbound requests from the Microsoft cloud over ExpressRoute.

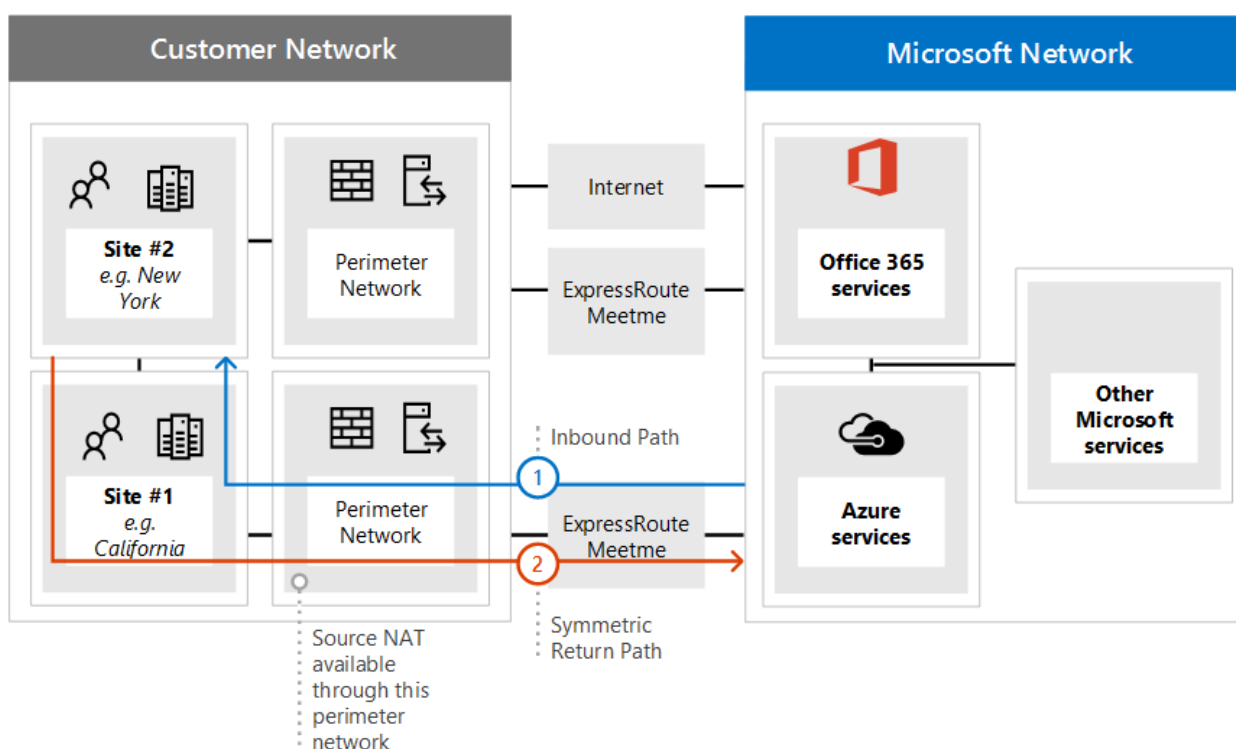
1. The inbound request from Office 365 retrieves the IP address from DNS and sends the request to your perimeter network.
 2. In this faulty configuration, there is no Source NAT configured or available at the perimeter network where the traffic is sent resulting in the actual source IP address being used as the return destination.
- The computer on your network routes the return traffic to Office 365 through any available ExpressRoute network connection.
 - The result is an Asymmetric connection to Office 365.



Solution 2: Source NAT

Simply adding a source NAT to the inbound request resolves this misconfigured network. In this diagram:

1. The incoming request continues to enter through the New York data center's perimeter network. This time Source NAT is available.
2. The response from the server routes back toward the IP associated with the Source NAT instead of the original IP address, resulting in the response returning along the same network path.



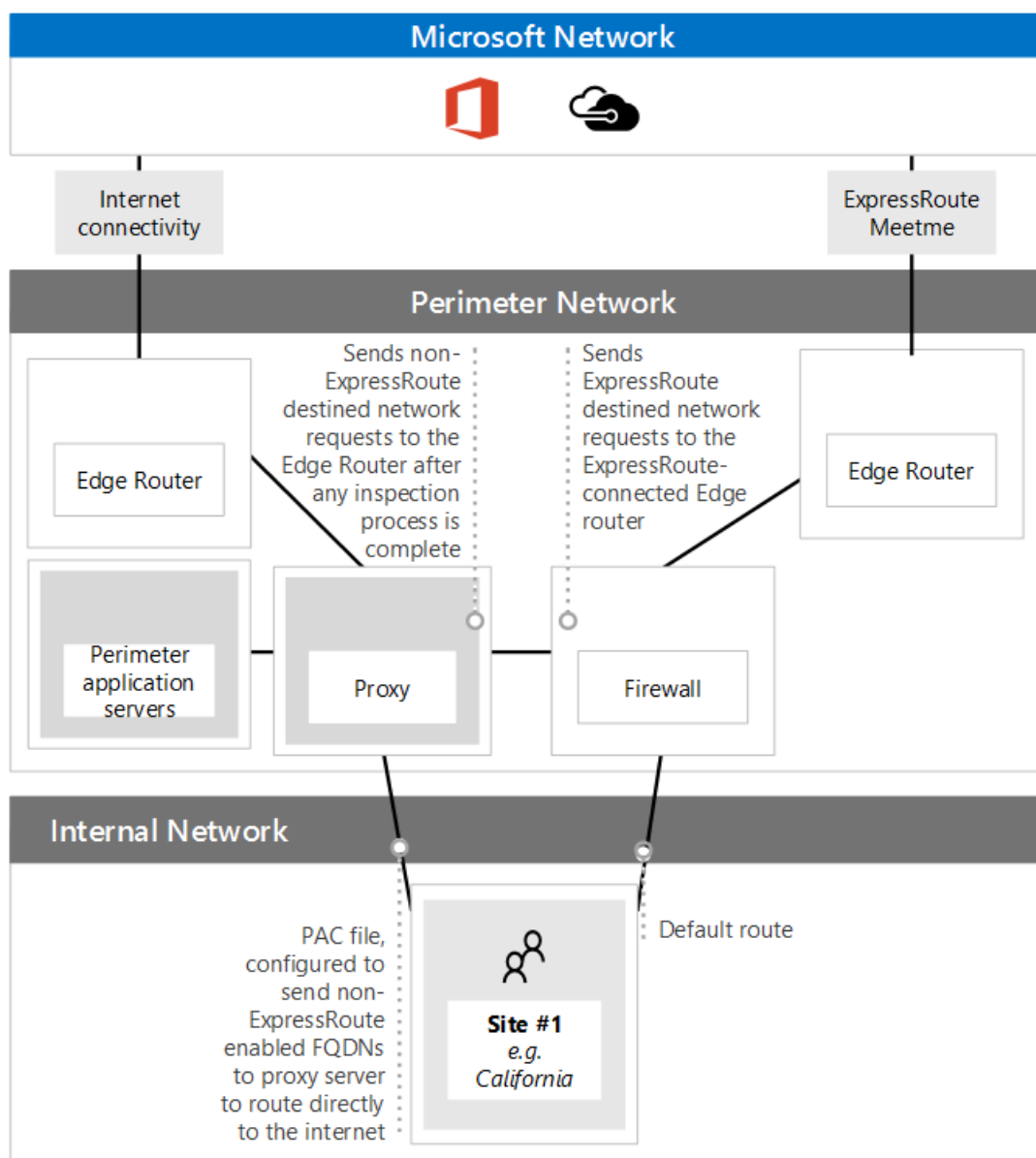
Paper verify that the network design has path symmetry

At this point, you need to verify on paper that your implementation plan offers route symmetry for the different scenarios in which you'll be using Office 365. You'll identify the specific network route that is expected to be taken when a person uses different features of the service. From the on-premises network and WAN routing, to the perimeter devices, to the connectivity path; ExpressRoute or the internet, and on to the connection to the online endpoint.

You'll need to do this for all of the Office 365 network services that were previously identified as services that your organization will adopt.

It helps to do this paper walk-through of routes with a second person. Explain to them where each network hop is expected to get its next route from and ensure that you're familiar with the routing paths. Remember that ExpressRoute will always provide a more scoped route to Microsoft server IP addresses giving it lower route cost than an Internet default route.

Design Client Connectivity Configuration



If you're using a proxy server for internet bound traffic, then you need to adjust any PAC or client configuration files to ensure client computers on your network are correctly configured to send the ExpressRoute traffic you desire to Office 365 without transiting your proxy server, and the remaining traffic, including some Office 365 traffic, is sent to the relevant proxy. Read our guide on [managing Office 365 endpoints](#), for example, PAC files.

NOTE

The endpoints change frequently, as often as weekly. You should only make changes based on the services and features your organization has adopted to reduce the number of changes you'll need to make to stay current. Pay close attention to the **Effective Date** in the RSS feed where the changes are announced and a record is kept of all past changes, IP addresses that are announced may not be advertised, or removed from advertisement, until the effective date is reached.

Build your deployment and testing procedures

Your implementation plan should include both testing and rollback planning. If your implementation isn't functioning as expected, the plan should be designed to affect the least number of people before problems are discovered. The following are some high-level principles your plan should consider.

1. Stage the network segment and user service onboarding to minimize disruption.
2. Plan for testing routes with traceroute and TCP connect from a separate internet connected host.
3. Preferably, testing of inbound and outbound services should be done on an isolated test network with a test Office 365 tenant.
 - Alternatively, testing can be performed on a production network if the customer is not yet using Office 365 or is in pilot.
 - Alternatively, testing can be performed during a production outage that is set aside for test and monitoring only.
 - Alternatively, testing can be done by checking routes for each service on each layer 3 router node. This fall back should only be used if no other testing is possible since a lack of physical testing introduces risk.

Build your deployment procedures

Your deployment procedures should roll out to small groups of people in stages to allow for testing before deploying to larger groups of people. The following are several ways to stage the deployment of ExpressRoute.

1. Set up ExpressRoute with Microsoft peering and have the route advertisements forwarded to a single host only for staged testing purposes.
2. Advertise routes to the ExpressRoute network to a single network segment at first and expand route advertisements by network segment or region.
3. If deploying Office 365 for the first time, use the ExpressRoute network deployment as a pilot for a few people.
4. If using proxy servers, you can alternatively configure a test PAC file to direct a few people to ExpressRoute with testing and feedback before adding more.

Your implementation plan should list each of the deployment procedures that must be taken or commands that need to be used to deploy the networking configuration. When the network outage time arrives, all of the changes being made should be from the written deployment plan that was written in advance and peer reviewed. See our guidance on the technical configuration of ExpressRoute.

- Updating your SPF TXT records if you've changed IP addresses for any on-premises servers that will continue to send email.
- Updating any DNS entries for on-premises servers if you've changed IP addresses to accommodate a new NAT configuration.
- Ensure you've subscribed to the RSS feed for Office 365 endpoint notifications to maintain any routing or proxy configurations.

After your ExpressRoute deployment is complete, the procedures in the test plan should be executed. Results for each procedure should be logged. You must include procedures for rolling back to the original production environment in the event the test plan results indicate the implementation was not successful.

Build your test procedures

Your testing procedures should include tests for each outbound and inbound network service for Office 365 both that will be using ExpressRoute and ones that will not. The procedures should include testing from each unique network location including users who are not on-premises in the corporate LAN.

Some examples of test activities include the following.

1. Ping from your on-premises router to your network operator router.
2. Validate the 500+ Office 365 and CRM Online IP address advertisements are received by your on-premises router.
3. Validate your inbound and outbound NAT is operating between ExpressRoute and the internal network.
4. Validate that routes to your NAT are being advertised from your router.
5. Validate that ExpressRoute has accepted your advertised prefixes.
 - Use the following cmdlet to verify peering advertisements:

```
Get-AzureRmExpressRouteCircuitRouteTable -DevicePath Primary -ExpressRouteCircuitName TestER -ResourceGroupName RG -PeeringType MicrosoftPeering
```

6. Validate your public NAT IP range is not advertised to Microsoft through any other ExpressRoute or public Internet network circuit unless it is a specific subset of a larger range as in the previous example.
7. ExpressRoute circuits are paired, validate that both BGP sessions are running.
8. Set up a single host on the inside of your NAT and use ping, tracert, and tcping to test connectivity across the new circuit to the host outlook.office365.com. Alternatively, you could use a tool such as Wireshark or Microsoft Network Monitor 3.4 on a mirrored port to the MSEE to validate you're able to connect to the IP address associated with outlook.office365.com.
9. Test application level functionality for Exchange Online.
 - Test Outlook is able to connect to Exchange Online and send/receive email.
 - Test Outlook is able to use online-mode.
 - Test smartphone connectivity and send/receive capability.
10. Test application level functionality for SharePoint Online
 - Test OneDrive for Business sync client.
 - Test SharePoint Online web access.
11. Test application level functionality for Skype for Business calling scenarios:
 - Join to conference call as authenticated user [invite initiated by end user].
 - Invite user to conference call [invite sent from MCU].
 - Join conference as anonymous user using the Skype for Business web application.
 - Join call from your wired PC connection, IP phone, and mobile device.
 - Call to federated user o Call to PSTN Validation: call is completed, call quality is acceptable, connection time is acceptable.
 - Verify presence status for contacts is updated for both members of the tenant and federated users.

Common problems

Asymmetric routing is the most common implementation problem. Here are some common sources to look for:

- Using an open or flat network routing topology without source NAT in place.

- Not using SNAT to route to inbound services through both the internet and ExpressRoute connections.
- Not testing inbound services on ExpressRoute on a test network prior to deploying broadly.

Deploying ExpressRoute connectivity through your network

Stage your deployment to one segment of the network at a time, progressively rolling out the connectivity to different parts of the network with a plan to roll back for each new network segment. If your deployment is aligned with an Office 365 deployment, deploy to your Office 365 pilot users first and extend from there.

First for your test and then for production:

- Run the deployment steps to enable ExpressRoute.
- Test your seeing the network routes are as expected.
- Perform testing on each inbound and outbound service.
- Rollback if you discover any issues.

Set up a test connection to ExpressRoute with a test network segment

Now that you have the completed plan on paper it is time to test at a small scale. In this test you will establish a single ExpressRoute connection with Microsoft Peering to a test subnet on your on-premises network. You can configure a [trial Office 365 tenant](#) with connectivity to and from the test subnet and include all outbound and inbound services that you will be using in production in the test subnet. Set up DNS for the test network segment and establish all inbound and outbound services. Execute your test plan and ensure that you are familiar with the routing for each service and the route propagation.

Execute the deployment and test plans

As you complete the items described above, check off the areas you've completed and ensure you and your team have reviewed them before executing your deployment and testing plans.

- List of outbound and inbound services that are involved in the network change.
- Global network architecture diagram showing both internet egress and ExpressRoute meet-me locations.
- Network routing diagram demonstrating the different network paths used for each service deployed.
- A deployment plan with steps to implement the changes and rollback if needed.
- A test plan for testing each Office 365 and network service.
- Completed paper validation of production routes for inbound and outbound services.
- A completed test across a test network segment including availability testing.

Choose an outage window that is long enough to run through the entire deployment plan and the test plan, has some time available for troubleshooting and time for rolling back if necessary.

Caution

Due to the complex nature of routing over both the internet and ExpressRoute, it is recommended that additional buffer time is added to this window to handle troubleshooting complex routing.

Configure QoS for Skype for Business Online

QoS is necessary to obtain voice and meeting benefits for Skype for Business Online. You can configure QoS after you have ensured that the ExpressRoute network connection does not block any of your other Office 365 service access. Configuration for QoS is described in the article [ExpressRoute and QoS in Skype for Business Online](#).

Troubleshooting your implementation

The first place to look is at the steps in this implementation guide, were any missed in your implementation plan? Go back and run further small network testing if possible to replicate the error and debug it there.

Identify which inbound or outbound services failed during testing. Get specifically the IP addresses and subnets for each of the services that failed. Go ahead and walk the network topology diagram on paper and validate the routing. Validate specifically where the ExpressRoute routing is advertised to, Test that routing during the outage if possible with traces.

Run PSPing with a network trace to each customer endpoint and evaluate source and destination IP addresses to validate that they are as expected. Run telnet to any mail host that you expose on port 25 and verify that SNAT is hiding the original source IP address if this is expected.

Keep in mind that while deploying Office 365 with an ExpressRoute connection you'll need to ensure both the network configuration for ExpressRoute is optimally designed and you've also optimized the other components on your network such as client computers. In addition to using this planning guide to troubleshoot the steps you may have missed, we also have written a [Performance troubleshooting plan for Office 365](#) .

Here's a short link you can use to come back: <https://aka.ms/implementexpressroute365>

Related Topics

[Assessing Office 365 network connectivity](#)

[Azure ExpressRoute for Office 365](#)

[Managing ExpressRoute for Office 365 connectivity](#)

[Routing with ExpressRoute for Office 365](#)

[Network planning with ExpressRoute for Office 365](#)

[Using BGP communities in ExpressRoute for Office 365 scenarios](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Optimizing your network for Skype for Business Online](#)

[ExpressRoute and QoS in Skype for Business Online](#)

[Call flow using ExpressRoute](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 network and performance tuning](#)

Routing with ExpressRoute for Office 365

10/28/2022 • 15 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

To properly understand routing traffic to Office 365 using Azure ExpressRoute, you'll need a firm grasp of the core [ExpressRoute routing requirements](#) and the [ExpressRoute circuits and routing domains](#). These lay out the fundamentals for using ExpressRoute that Office 365 customers will rely on.

Some of the key items in the above articles that you'll need to understand include:

- ExpressRoute circuits aren't mapped to specific physical infrastructure, but are a logical connection made at a single peering location by Microsoft and a peering provider on your behalf.
- There's a 1:1 mapping between an ExpressRoute circuit and a customer s-key.
- Each circuit can support two independent peering relationships (Azure Private peering, and Microsoft peering); Office 365 requires Microsoft peering.
- Each circuit has a fixed bandwidth that is shared across all peering relationships.
- Any public IPv4 addresses and public AS numbers that will be used for the ExpressRoute circuit must be validated as being owned by you, or assigned exclusively to you by the owner of the address range.
- The virtual ExpressRoute circuits are redundant globally and will follow standard BGP routing practices. This is why we recommend two physical circuits per egress to your provider in an active/active configuration.

See the [FAQ page](#) for more information on services supported, costs, and configuration details. See the [ExpressRoute locations article](#) for information on the list of connectivity providers offering Microsoft peering support. We've also recorded a 10-part [Azure ExpressRoute for Office 365 Training](#) series on Channel 9 to help explain the concepts more thoroughly.

Ensuring route symmetry

The Office 365 front-end servers are accessible on both the Internet and ExpressRoute. These servers will prefer to route back to on-premises over ExpressRoute circuits when both are available. Because of this, there is a possibility of route asymmetry if traffic from your network prefers to route over your Internet circuits. Asymmetrical routes are a problem because devices that perform stateful packet inspection can block return traffic that follows a different path than the outbound packets followed.

Regardless of whether you initiate a connection to Office 365 over the Internet or ExpressRoute, the source must be a publicly routable address. With many customers peering directly with Microsoft, having private addresses where duplication is possible between customers isn't feasible.

The following are scenarios where communications from Office 365 to your on-premises network will be initiated. To simplify your network design, we recommend routing the following over the Internet path.

- SMTP services such as mail from an Exchange Online tenant to an on-premises host or SharePoint Online Mail sent from SharePoint Online to an on-premises host. SMTP protocol is used more broadly within Microsoft's network than the route prefixes shared over ExpressRoute circuits and advertising on-premises SMTP servers over ExpressRoute will cause failures with these other services.
- ADFS during password validation for signing in.

- [Exchange Server Hybrid deployments.](#)
- [SharePoint federated hybrid search.](#)
- [SharePoint hybrid BCS.](#)
- [Skype for Business hybrid](#) and/or [Skype for Business federation.](#)
- [Skype for Business Cloud Connector.](#)

For Microsoft to route back to your network for these bi-directional traffic flows, the BGP routes to your on-premises devices must be shared with Microsoft. When you advertise route prefixes to Microsoft over ExpressRoute, you should follow these best practices:

1. Do not advertise the same public IP Address route prefix to the public Internet and over ExpressRoute. It is recommended that the IP BGP Route Prefix advertisements to Microsoft over ExpressRoute are from a range that is not advertised to the internet at all. If this is not possible to achieve due to the available IP Address space, then it is essential to ensure you advertise a more specific range over ExpressRoute than any internet circuits.
2. Use separate NAT IP pools per ExpressRoute circuit and separate to that of your internet circuits.
3. Any route advertised to Microsoft will attract network traffic from any server in Microsoft's network, not only those for which routes are advertised to your network over ExpressRoute. Only advertise routes to servers where routing scenarios are defined and well understood by your team. Advertise separate IP Address route prefixes at each of multiple ExpressRoute circuits from your network.

Deciding which applications and features route over ExpressRoute

When you configure a peering relationship using the Microsoft peering routing domain and are approved for the appropriate access, you'll be able to see all PaaS and SaaS services available over ExpressRoute. The Office 365 services designed for ExpressRoute can be managed with [BGP communities](#) or [route filters](#).

Each of the Office 365 features that are available using Microsoft peering are listed in the [Office 365 endpoints article](#) by application type and FQDN. The reason for using the FQDN in the tables is to allow customers to manage traffic using PAC files or other proxy configurations, see our guide to [managing Office 365 endpoints](#) for example PAC files.

In some situations we've used a wildcard domain where one or more sub-FQDNs are advertised differently than the higher-level wildcard domain. It usually happens when the wildcard represents a long list of servers that are all advertised to ExpressRoute and the Internet, while a small subset of destinations is only advertised to the Internet, or the reverse. Refer to the tables below to understand where the differences are.

This table displays the wildcard FQDNs that are advertised to both the internet and Azure ExpressRoute alongside the sub-FQDNs that are advertised only to the internet.

WILDCARD DOMAIN ADVERTISED TO EXPRESSROUTE AND INTERNET CIRCUITS	SUB-FQDN ADVERTISED TO INTERNET CIRCUITS ONLY
*.microsoftonline.com	click.email.microsoftonline.com portal.microsoftonline.com provisioningapi.microsoftonline.com adminwebservice.microsoftonline.com

WILDCARD DOMAIN ADVERTISED TO EXPRESSROUTE AND INTERNET CIRCUITS	SUB-FQDN ADVERTISED TO INTERNET CIRCUITS ONLY
*.officeapps.live.com	nexusRules.officeapps.live.com nexus.officeapps.live.com odc.officeapps.live.com odc.officeapps.live.com cdn.odc.officeapps.live.com ols.officeapps.live.com ocsredir.officeapps.live.com ocws.officeapps.live.com ocsa.officeapps.live.com

Usually PAC files are intended to send network requests to ExpressRoute advertised endpoints directly to the circuit and all other network requests to your proxy. If you're configuring a PAC file like this, compose your PAC file in the following order:

1. Include the sub-FQDNs from column two in the above table at the top of your PAC file, sending the traffic towards your proxy. We've built a sample PAC file for you to use in our article on [managing Office 365 endpoints](#).
2. Include all FQDNs marked advertised to ExpressRoute in [this article](#) below the first section, sending the traffic directly to your ExpressRoute circuit.
3. Include any other network endpoints or rules below these two entries, sending the traffic towards your proxy.

This table displays the wildcard domains that are advertised to Internet circuits only alongside the sub-FQDNs that are advertised to Azure ExpressRoute and Internet circuits. For your PAC file above, the FQDNs in column 2 in the below table are listed as being advertised to ExpressRoute in the link referenced, which means they would be included in the second group of entries in the file.

WILDCARD DOMAIN ADVERTISED TO INTERNET CIRCUITS ONLY	SUB-FQDN ADVERTISED TO EXPRESSROUTE AND INTERNET CIRCUITS
*.office.com	*.outlook.office.com home.office.com outlook.office.com portal.office.com www.office.com
*.office.net	agent.office.net
*.office365.com	outlook.office365.com smtp.office365.com
*.outlook.com	*.protection.outlook.com *.mail.protection.outlook.com autodiscover- <tenant>.outlook.com
*.windows.net	login.windows.net

Routing Office 365 traffic over the Internet and ExpressRoute

To route to the Office 365 application of your choosing, you'll need to determine a number of key factors.

1. How much bandwidth the application will require. Sampling existing usage is the only reliable method for determining this in your organization.

2. What egress location(s) you want the network traffic to leave your network from. You should plan to minimize the network latency for connectivity to Office 365 as this will impact performance. Because Skype for Business uses real-time voice and video, it is susceptible to poor network latency.
3. If you want all or a subset of your network locations to use ExpressRoute.
4. What locations your chosen network provider offers ExpressRoute from.

Once you determine the answers to these questions, you can provision an ExpressRoute circuit that meets the bandwidth and location needs. For more network planning assistance, refer to the [Office 365 network tuning guide](#) and the [case study on how Microsoft handles network performance planning](#).

Example 1: Single geographic location

This example is a scenario for a fictitious company called Trey Research who has a single geographic location.

Employees at Trey Research are only allowed to connect to the services and websites on the internet that the security department explicitly allows on the pair of outbound proxies that sit between the corporate network and their ISP.

Trey Research plans to use Azure ExpressRoute for Office 365 and recognizes that some traffic such as traffic destined for content delivery networks won't be able to route over the ExpressRoute for Office 365 connection. Since all traffic already routes to the proxy devices by default, these requests will continue to work as before. After Trey Research determines they can meet the Azure ExpressRoute routing requirements, they proceed to create a circuit, configure routing, and linking the new ExpressRoute circuit to a virtual network. Once the fundamental Azure ExpressRoute configuration is in place, Trey Research uses the [#2 PAC file we publish](#) to route traffic with customer-specific data over the direct ExpressRoute for Office 365 connections.

As shown in the following diagram, Trey Research is able to satisfy the requirement to route Office 365 traffic over the internet and a subset of traffic over ExpressRoute using a combination of routing and outbound proxy configuration changes.

1. Using the [#2 PAC file we publish](#) to route traffic through a separate internet egress point for Azure ExpressRoute for Office 365.
2. Clients are configured with a default route towards Trey Research's proxies.

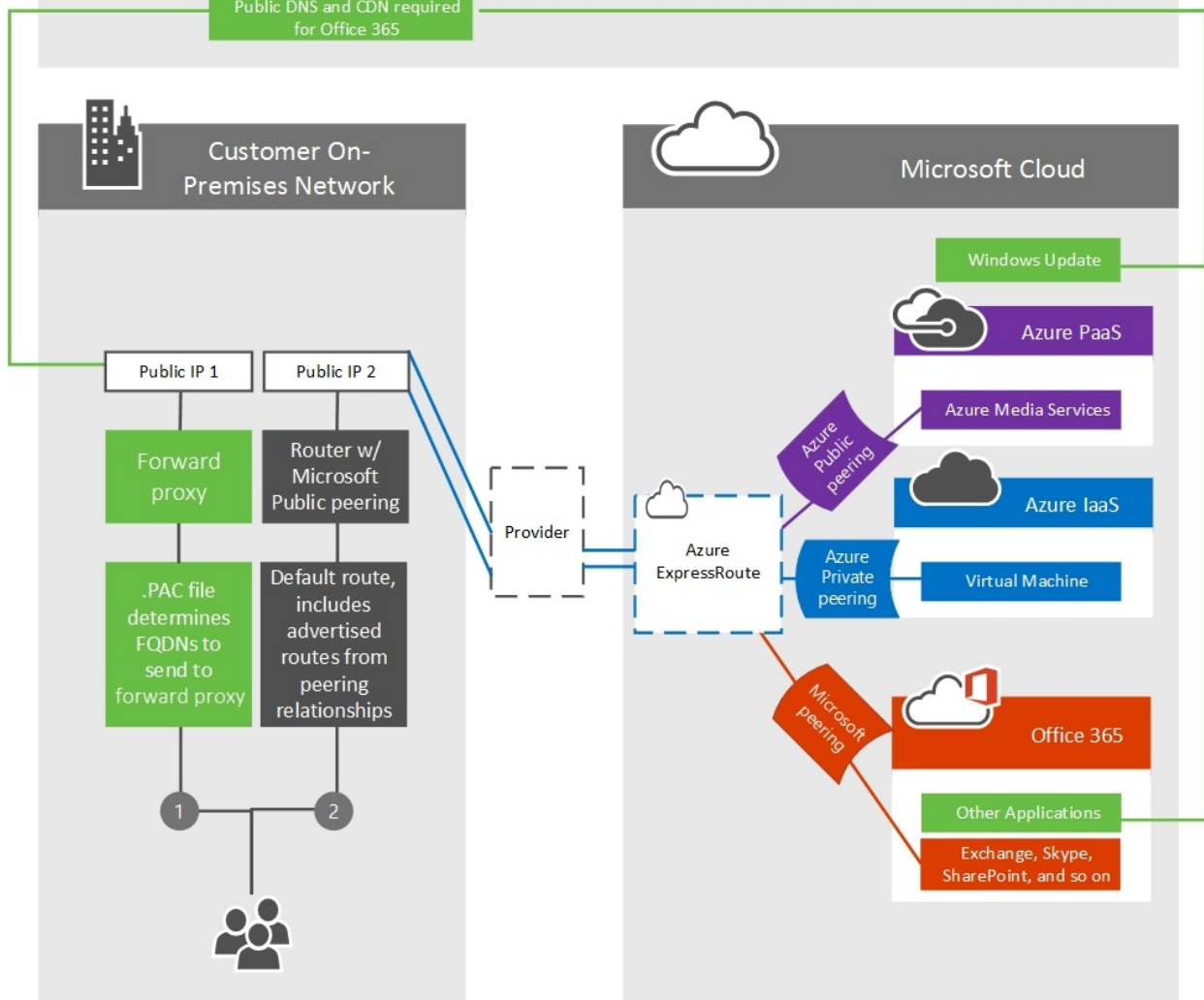
In this example scenario, Trey Research is using an outbound proxy device. Similarly, customers who aren't using Azure ExpressRoute for Office 365 may want to use this technique to route traffic based on the cost of inspecting traffic destined for well-known high volume endpoints.

The highest volume FQDNs for Exchange Online, SharePoint Online, and Skype for Business Online are the following:



Public Internet

Public DNS and CDN required
for Office 365



- outlook.office365.com, outlook.office.com
- <tenant-name>.sharepoint.com, <tenant-name>-my.sharepoint.com, <tenant-name>-<app>.sharepoint.com
- *.Lync.com along with the IP ranges for non-TCP traffic
- *broadcast.officeapps.live.com, *excel.officeapps.live.com, *onenote.officeapps.live.com, *powerpoint.officeapps.live.com, *view.officeapps.live.com, *visio.officeapps.live.com, *word-edit.officeapps.live.com, *word-view.officeapps.live.com, office.live.com

Learn more about [deploying and managing proxy settings in Windows 8](#) and [ensuring Office 365 isn't throttled by your proxy](#).

With a single ExpressRoute circuit, there is no high availability for Trey Research. In the event Trey's redundant pair of edge devices that are servicing the ExpressRoute connectivity fail, there is not an extra ExpressRoute circuit to fail over to. This leaves Trey Research in a predicament as failing over to the internet will require manual reconfiguration and in some cases new IP addresses. If Trey wants to add high availability, the simplest solution is to add extra ExpressRoute circuits for each location and configure the circuits in an active/active manner.

Routing ExpressRoute for Office 365 with multiple locations

The last scenario, routing Office 365 traffic over ExpressRoute is the foundation for even more complex routing

architecture. Regardless of the number of locations, number of continents where those locations exist, number of ExpressRoute circuits, and so on, being able to route some traffic to the Internet and some traffic over ExpressRoute will be required.

The extra questions that must be answered for customers with multiple locations in multiple geographies include:

1. Do you require an ExpressRoute circuit in every location? If you're using Skype for Business Online or are concerned with latency sensitivity for SharePoint Online or Exchange Online, a redundant pair of active/active ExpressRoute circuits is recommended in each location. See the Skype for Business media quality and network connectivity guide for more details.
2. If an ExpressRoute circuit isn't available in a particular region, how should Office 365 destined traffic be routed?
3. What is the preferred method for consolidating traffic in the case of networks with many small locations?

Each of these presents a unique challenge that requires you to evaluate your own network and the options available from Microsoft.

CONSIDERATION	NETWORK COMPONENTS TO EVALUATE
Circuits in more than one location	We recommend a minimum of two circuits configured in an active/active manner. Cost, latency, and bandwidth needs must be compared. Use BGP route cost, PAC files, and NAT to manage routing with multiple circuits.
Routing from locations without an ExpressRoute circuit	We recommend egress and DNS resolution as close to the person initiating the request for Office 365. DNS forwarding can be used to allow remote offices to discover the appropriate endpoint. Clients in the remote office must have a route available that provides access to the ExpressRoute circuit.
Small office consolidation	Available bandwidth and data usage should be carefully compared.

NOTE

Microsoft will prefer ExpressRoute over the internet if the route is available regardless of physical location.

Each of these considerations must be taken into account for each unique network. Below is an example.

Example 2: Multi-geographic locations

This example is a scenario for a fictitious company called 'Humongous Insurance' who has multiple geographic locations.

Humongous Insurance is geographically dispersed with offices all over the world. They want to implement Azure ExpressRoute for Office 365 to keep most their Office 365 traffic on direct network connections. Humongous Insurance also has offices on two additional continents. The employees in the remote office where ExpressRoute is not feasible will need to route back to one or both of the primary facilities to use an ExpressRoute connection.

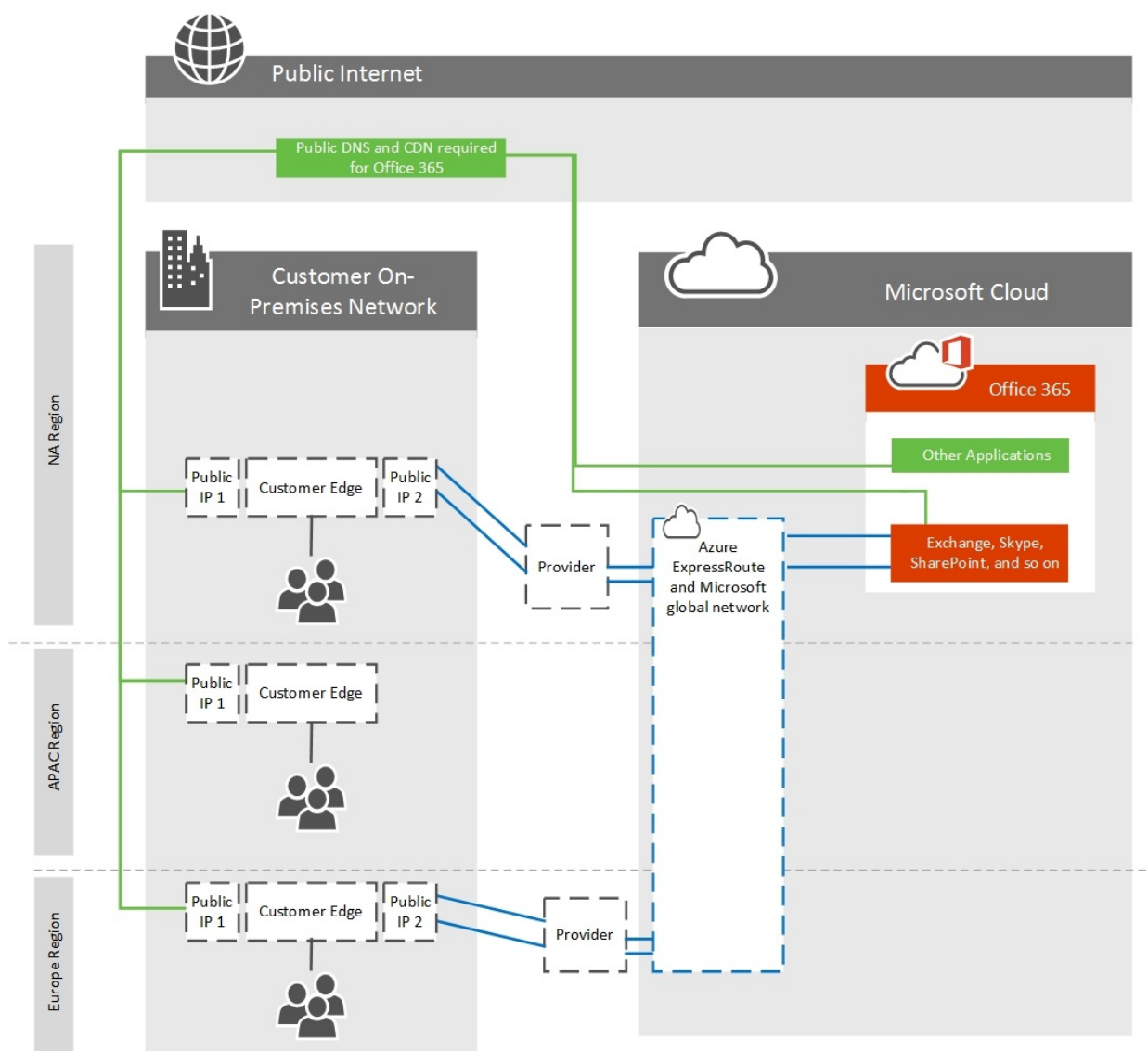
The guiding principle is to get Office 365 destined traffic to a Microsoft datacenter as quickly as possible. In this example, Humongous Insurance must decide if their remote offices should route over the Internet to get to a Microsoft datacenter over any connection as quickly as possible or if their remote offices should route over an

internal network to get to a Microsoft datacenter over an ExpressRoute connection as quickly as possible.

Microsoft's datacenters, networks, and application architecture are designed to take globally disparate communications and service them in the most efficient way possible. This is one of the largest networks in the world. Requests destined for Office 365 that remain on customer networks longer than necessary won't be able to take advantage of this architecture.

In Humongous Insurance's situation, they should proceed depending on the applications they intend to use over ExpressRoute. For example, if they're a Skype for Business Online customer, or plan to use ExpressRoute connectivity when connecting to external Skype for Business Online meetings, the design recommended in the Skype for Business Online media quality and network connectivity guide is to provision an additional ExpressRoute circuit for the third location. This may be more expensive from a networking perspective; however, routing requests from one continent to another before delivering to a Microsoft datacenter may cause a poor or unusable experience during Skype for Business Online meetings and communications.

If Humongous Insurance isn't using or doesn't plan to use Skype for Business Online in any way, routing Office 365 destined network traffic back to a continent with an ExpressRoute connection may be feasible though may cause unnecessary latency or TCP congestion. In both cases, routing Internet destined traffic to the Internet at the local site is recommended to take advantage of the content delivery networks that Office 365 relies on.



When Humongous Insurance is planning their multi-geography strategy, there are many things to consider around size of circuit, number of circuits, failover, and so on.

With ExpressRoute in a single location with multiple regions attempting to use the circuit, Humongous Insurance wants to ensure that connections to Office 365 from the remote office are sent to the Office 365 datacenter

nearest headquarters and received by the headquarters location. To do this, Humongous Insurance implements DNS forwarding to reduce the number of round trips and DNS lookups required to establish the appropriate connection with the Office 365 environment closest to the headquarters internet egress point. This prevents the client from resolving a local front-end server and ensures the Front-End server the person connects to be near the headquarters where Humongous Insurance is peering with Microsoft. You can also learn to [Assign a Conditional Forwarder for a Domain Name](#).

In this scenario, traffic from the remote office would resolve the Office 365 front-end infrastructure in North America and use Office 365 to connect to the backend servers according to the architecture of the Office 365 application. For example, Exchange Online would terminate the connection in North America and those front-end servers would connect to the backend mailbox server wherever the tenant resided. All services have a widely distributed front door service comprised of unicast and anycast destinations.

If Humongous has major offices in multiple continents, a minimum of two active/active circuits per region are recommended in order to reduce latency for sensitive applications such as Skype for Business Online. If all offices are in a single continent, or is not using real-time collaboration, having a consolidated or distributed egress point is a customer-specific decision. When multiple circuits are available, BGP routing will ensure failover should any single circuit become unavailable.

Learn more about sample [routing configurations](#) and <https://azure.microsoft.com/documentation/articles/expressroute-config-samples-nat/>.

Selective routing with ExpressRoute

Selective routing with ExpressRoute may be needed for various reasons, such as testing, rolling out ExpressRoute to a subset of users. There are various tools customers can use to selectively route Office 365 network traffic over ExpressRoute:

1. **Route filtering/segregation** - allowing the BGP routes to Office 365 over ExpressRoute to a subset of your subnets or routers. This selectively routes by customer network segment or physical office location. This is common for staggering rollout of ExpressRoute for Office 365 and is configured on your BGP devices.
2. **PAC files/URLs** - directing Office 365 destined network traffic for specific FQDNs to route on a specific path. This selectively routes by client computer as identified by [PAC file deployment](#).
3. **Route filtering** - [Route filters](#) are a way to consume a subset of supported services through Microsoft peering.
4. **BGP communities** - filtering based on [BGP community tags](#) allows a customer to determine which Office 365 applications will traverse ExpressRoute and which will traverse the internet.

Here's a short link you can use to come back: <https://aka.ms/erorouting>

Related Topics

[Assessing Office 365 network connectivity](#)

[Azure ExpressRoute for Office 365](#)

[Managing ExpressRoute for Office 365 connectivity](#)

[Network planning with ExpressRoute for Office 365](#)

[Implementing ExpressRoute for Office 365](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Optimizing your network for Skype for Business Online](#)

[ExpressRoute and QoS in Skype for Business Online](#)

[Call flow using ExpressRoute](#)

[Using BGP communities in ExpressRoute for Office 365 scenarios](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 network and performance tuning](#)

Microsoft 365 endpoints

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Endpoints are the set of destination IP addresses, DNS domain names, and URLs for Microsoft 365 traffic on the Internet.

To optimize performance to Microsoft 365 cloud-based services, these endpoints need special handling by your client browsers and the devices in your edge network. These devices include firewalls, SSL Break and Inspect and packet inspection devices, and data loss prevention systems.

See [Managing Microsoft 365 endpoints](#) for the details.

There are currently five different Microsoft 365 clouds. This table takes you to the list of endpoints for each one.

CLOUD	DESCRIPTION
Worldwide endpoints	The endpoints for worldwide Microsoft 365 subscriptions, which include the United States Government Community Cloud (GCC).
U.S. Government DoD endpoints	The endpoints for United States Department of Defense (DoD) subscriptions.
U.S. Government GCC High endpoints	The endpoints for United States Government Community Cloud High (GCC High) subscriptions.
Microsoft 365 operated by 21Vianet endpoints	The endpoints for Microsoft 365 operated by 21Vianet, which is designed to meet the needs for Microsoft 365 in China.

To automate getting the latest list of endpoints for your Microsoft 365 cloud, see the [Office 365 IP Address and URL Web service](#).

For additional endpoints, see these articles:

- [Additional endpoints not included in the Web service](#)
- [Network requests in Office 2016 for Mac](#)

If you are a network equipment vendor, join the [Office 365 Networking Partner Program](#). Enroll in the program to build Microsoft 365 network connectivity principles into your products and solutions.

Managing Office 365 endpoints

10/28/2022 • 14 minutes to read • [Edit Online](#)

Most enterprise organizations that have multiple office locations and a connecting WAN will need configuration for Office 365 network connectivity. You can optimize your network by sending all trusted Office 365 network requests directly through your firewall, bypassing all extra packet level inspection or processing. This reduces latency and your perimeter capacity requirements. Identifying Office 365 network traffic is the first step in providing optimal performance for your users. For more information, see [Office 365 Network Connectivity Principles](#).

Microsoft recommends you access the Office 365 network endpoints and ongoing changes to them using the [Office 365 IP Address and URL Web Service](#).

Regardless of how you manage vital Office 365 network traffic, Office 365 requires Internet connectivity. Other network endpoints where connectivity is required are listed at [Additional endpoints not included in the Office 365 IP Address and URL Web service](#).

How you use the Office 365 network endpoints will depend on your enterprise organization network architecture. This article outlines several ways that enterprise network architectures can integrate with Office 365 IP addresses and URLs. The easiest way to choose which network requests to trust is to use SD-WAN devices that support automated Office 365 configuration at each of your office locations.

SD-WAN for local branch egress of vital Office 365 network traffic

At each branch office location, you can provide an SD-WAN device that is configured to route traffic for Office 365 Optimize category of endpoints, or Optimize and Allow categories, directly to Microsoft's network. Other network traffic including on-premises datacenter traffic, general Internet web sites traffic, and traffic to Office 365 Default category endpoints is sent to another location where you have a more substantial network perimeter.

Microsoft is working with SD-WAN providers to enable automated configuration. For more information, see [Office 365 Networking Partner Program](#).

Use a PAC file for direct routing of vital Office 365 traffic

Use PAC or WPAD files to manage network requests that are associated with Office 365 but don't have an IP address. Typical network requests that are sent through a proxy or perimeter device increase latency. While SSL Break and Inspect creates the largest latency, other services such as proxy authentication and reputation lookup can cause poor performance and a bad user experience. Additionally, these perimeter network devices need enough capacity to process all of the network connection requests. We recommend bypassing your proxy or inspection devices for direct Office 365 network requests.

[PowerShell Gallery Get-PacFile](#) is a PowerShell script that reads the latest network endpoints from the Office 365 IP Address and URL Web service and creates a sample PAC file. You can modify the script so that it integrates with your existing PAC file management.

NOTE

For more information about the security and performance considerations of direct connectivity to Office 365 endpoints, see [Office 365 Network Connectivity Principles](#).

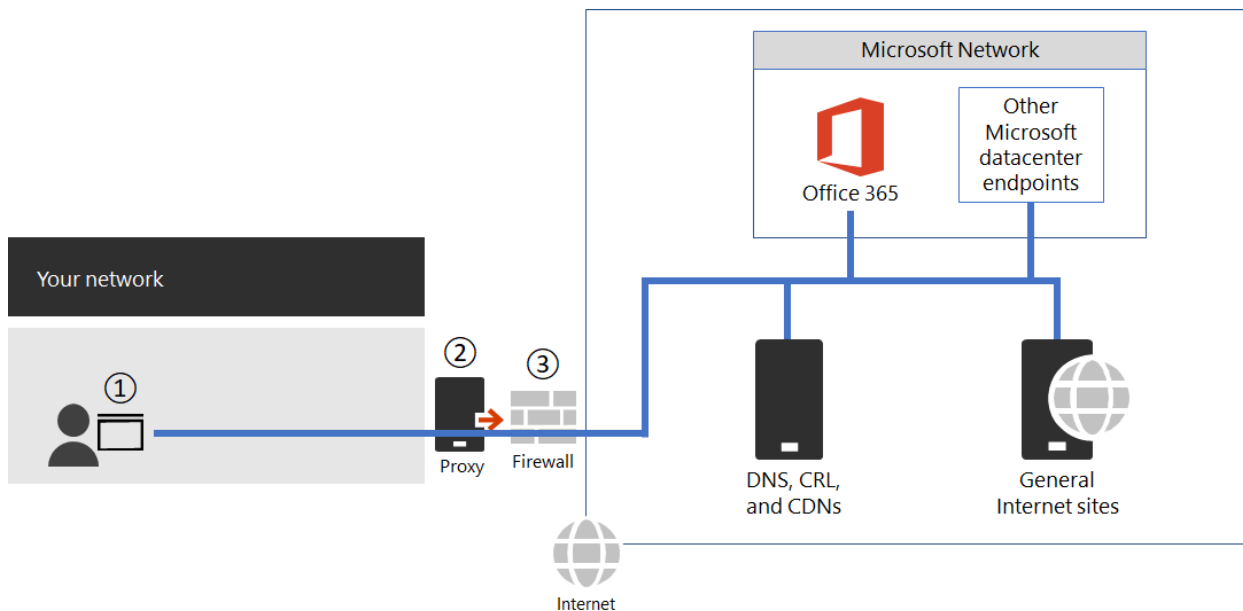


Figure 1 - Simple enterprise network perimeter

The PAC file is deployed to web browsers at point 1 in Figure 1. When using a PAC file for direct egress of vital Office 365 network traffic, you also need to allow connectivity to the IP addresses behind these URLs on your network perimeter firewall. This is done by fetching the IP addresses for the same Office 365 endpoint categories as specified in the PAC file and creating firewall ACLs based on those addresses. The firewall is point 3 in Figure 1.

Separately if you choose to only do direct routing for the Optimize category endpoints, any required Allow category endpoints that you send to the proxy server will need to be listed in the proxy server to bypass further processing. For example, SSL break and Inspect and Proxy Authentication are incompatible with both the Optimize and Allow category endpoints. The proxy server is point 2 in Figure 1.

The common configuration is to permit without processing all outbound traffic from the proxy server for the destination IP addresses for Office 365 network traffic that hits the proxy server. For information about issues with SSL Break and Inspect, see [Using third-party network devices or solutions on Office 365 traffic](#).

There are two types of PAC files that the Get-PacFile script will generate.

TYPE	DESCRIPTION
1	Send Optimize endpoint traffic direct and everything else to the proxy server.
2	Send Optimize and Allow endpoint traffic direct and everything else to the proxy server. This type can also be used to send all supported ExpressRoute for Office 365 traffic to ExpressRoute network segments and everything else to the proxy server.

Here's a simple example of calling the PowerShell script:

```
Get-PacFile -ClientId b10c5ed1-bad1-445f-b386-b919946339a7
```

There are many parameters you can pass to the script:

PARAMETER	DESCRIPTION
ClientRequestId	This is required and is a GUID passed to the web service that represents the client machine making the call.
Instance	The Office 365 service instance, which defaults to Worldwide. This is also passed to the web service.
TenantName	Your Office 365 tenant name. Passed to the web service and used as a replaceable parameter in some Office 365 URLs.
Type	The type of the proxy PAC file that you want to generate.

Here's another example of calling the PowerShell script with additional parameters:

```
Get-PacFile -Type 2 -Instance Worldwide -TenantName Contoso -ClientRequestId b10c5ed1-bad1-445f-b386-b919946339a7
```

Proxy server bypass processing of Office 365 network traffic

Where PAC files aren't used for direct outbound traffic, you still want to bypass processing on your network perimeter by configuring your proxy server. Some proxy server vendors have enabled automated configuration of this as described in the [Office 365 Networking Partner Program](#).

If you're doing this manually, you'll need to get the Optimize and Allow endpoint category data from the Office 365 IP Address and URL Web Service and configure your proxy server to bypass processing for these. It is important to avoid SSL Break and Inspect and Proxy Authentication for the Optimize and Allow category endpoints.

Change management for Office 365 IP addresses and URLs

In addition to selecting appropriate configuration for your network perimeter, it's critical that you adopt a change management process for Office 365 endpoints. These endpoints change regularly and if you don't manage the changes, you can end up with users blocked or with poor performance after a new IP address or URL is added.

Changes to the Office 365 IP addresses and URLs are usually published near the last day of each month. Sometimes a change will be published outside of that schedule due to operational, support, or security requirements.

When a change is published that requires you to act because an IP address or URL was added, you should expect to receive 30 days notice from the time we publish the change until there's an Office 365 service on that endpoint. This is reflected as the Effective Date. Although we aim for this notification period, it may not always be possible due to operational, support, or security requirements. Changes that don't require immediate action to maintain connectivity, such as removed IP addresses or URLs or less significant changes, don't include advance notification. In these instances, no Effective Date will be provided. Regardless of what notification is provided, we list the expected service active date for each change.

Change notification using the Web Service

You can use the Office 365 IP Address and URL Web Service to get change notification. We recommend you call the **/version** web method once an hour to check the version of the endpoints that you're using to connect to Office 365. If this version changes when compared to the version that you have in use, then you should get the latest endpoint data from the **/endpoints** web method and optionally get the differences from the **/changes**

web method. It isn't necessary to call the `/endpoints` or `/changes` web methods if there hasn't been any change to the version you found.

For more information, see [Office 365 IP Address and URL Web Service](#).

Change notification using RSS feeds

The Office 365 IP Address and URL Web Service provides an RSS feed that you can subscribe to in Outlook. There are links to the RSS URLs on each of the Office 365 service instance-specific pages for the IP addresses and URLs. For more information, see [Office 365 IP Address and URL Web Service](#).

Change notification and approval review using Power Automate

We understand that you might still require manual processing for network endpoint changes that come through each month. You can use Power Automate to create a flow that notifies you by email and optionally runs an approval process for changes when Office 365 network endpoints have changes. Once review is completed, you can have the flow automatically email the changes to your firewall and proxy server management team.

For information about a Power Automate sample and template, see [Use Power Automate to receive an email for changes to Office 365 IP addresses and URLs](#).

Office 365 network endpoints FAQ

See these frequently asked questions about Office 365 network connectivity.

How do I submit a question?

Click the link at the bottom to indicate if the article was helpful or not and submit any additional questions. We monitor the feedback and update the questions here with the most frequently asked.

How do I determine the location of my tenant?

Tenant location is best determined using our [datacenter map](#).

Am I peering appropriately with Microsoft?

Peering locations are described in more detail in [peering with Microsoft](#).

With over 2500 ISP peering relationships globally and 70 points of presence, getting from your network to ours should be seamless. It can't hurt to spend a few minutes making sure your ISP's peering relationship is the most optimal, [here's a few examples](#) of good and not so good peering hand-offs to our network.

I see network requests to IP addresses not on the published list, do I need to provide access to them?

We only provide IP addresses for the Office 365 servers you should route directly to. This isn't a comprehensive list of all IP addresses you'll see network requests for. You'll see network requests to Microsoft and third-party owned, unpublished, IP addresses. These IP addresses are dynamically generated or managed in a way that prevents timely notice when they change. If your firewall can't allow access based on the FQDNs for these network requests, use a PAC or WPAD file to manage the requests.

See an IP associated with Office 365 that you want more information on?

1. Check if the IP address is included in a larger published range using a CIDR calculator, such as these for [IPv4](#) or [IPv6](#). For example, 40.96.0.0/13 includes the IP Address 40.103.0.1 despite 40.96 not matching 40.103.
2. See if a partner owns the IP with a [whois query](#). If it's Microsoft owned, it may be an internal partner. Many partner network endpoints are listed as belonging to the *default* category, for which IP addresses aren't published.
3. The IP address may not be part of Office 365 or a dependency. Office 365 network endpoint publishing doesn't include all of Microsoft network endpoints.
4. Check the certificate. With a browser, connect to the IP address using `HTTPS://<IP_ADDRESS>` and check the

domains listed on the certificate to understand what domains are associated with the IP address. If it's a Microsoft-owned IP address and not on the list of Office 365 IP addresses, it's likely the IP address is associated with a Microsoft CDN such as *MSOCDN.NET* or another Microsoft domain without published IP information. If you do find the domain on the certificate is one where we claim to list the IP address, please let us know.

Some Office 365 URLs point to CNAME records instead of A records in the DNS. What do I have to do with the CNAME records?

Client computers need a DNS A or AAAA record that includes one or more IP address(es) to connect to a cloud service. Some URLs included in Office 365 show CNAME records instead of A or AAAA records. These CNAME records are intermediary and there may be several in a chain. They will always eventually resolve to an A or AAAA record for an IP Address. For example, consider the following series of DNS records, which ultimately resolves to the IP address *IP_1*:

```
serviceA.office.com -> CNAME: serviceA.domainA.com -> CNAME: serviceA.domainB.com -> A: IP_1
```

These CNAME redirects are a normal part of the DNS and are transparent to the client computer and transparent to proxy servers. They are used for load balancing, content delivery networks, high availability, and service incident mitigation. Microsoft doesn't publish the intermediary CNAME records, they are subject to change at any time, and you shouldn't need to configure them as allowed in your proxy server.

A proxy server validates the initial URL, which in the above example is *serviceA.office.com*, and this URL would be included in Office 365 publishing. The proxy server requests DNS resolution of that URL to an IP Address and will receive back *IP_1*. It doesn't validate the intermediary CNAME redirection records.

Hard-coded configurations or using an allowlist based on indirect Office 365 FQDNs aren't recommended, not supported by Microsoft, and are known to cause customer connectivity issues. DNS solutions that block on CNAME redirection, or that otherwise incorrectly resolve Office 365 DNS entries, can be solved via DNS forwarders with DNS recursion enabled or by using DNS root hints. Many third-party network perimeter products natively integrate recommended Office 365 endpoint to include an allowlist in their configuration using the [Office 365 IP Address and URL Web service](#).

Why do I see names such as *nsatc.net* or *akadns.net* in the Microsoft domain names?

Office 365 and other Microsoft services use several third-party services such as Akamai and MarkMonitor to improve your Office 365 experience. To keep giving you the best experience possible, we may change these services in the future. Third-party domains may host content, such as a CDN, or they may host a service, such as a geographical traffic management service. Some of the services currently in use include:

[MarkMonitor](#) is in use when you see requests that include **.nsatc.net*. This service provides domain name protection and monitoring to protect against malicious behavior.

[ExactTarget](#) is in use when you see requests to **.exacttarget.com*. This service provides email link management and monitoring against malicious behavior.

[Akamai](#) is in use when you see requests that include one of the following FQDNs. This service offers geo-DNS and content delivery network services.


```
*.akadns.net
*.akam.net
*.akamai.com
*.akamai.net
*.akamaiedge.net
*.akamaihd.net
*.akamaized.net
*.edgekey.net
*.edgesuite.net
```

I have to have the minimum connectivity possible for Office 365

As Office 365 is a suite of services built to function over the internet, the reliability and availability promises are based on many standard internet services being available. For example, standard internet services such as DNS, CRL, and CDNs must be reachable to use Office 365 just as they must be reachable to use most modern internet services.

The Office 365 suite is broken down into major service areas. These can be selectively enabled for connectivity and there's a Common area, which is a dependency for all and is always required.

SERVICE AREA	DESCRIPTION
Exchange	Exchange Online and Exchange Online Protection
SharePoint	SharePoint Online and OneDrive for Business
Skype for Business Online and Microsoft Teams	Skype for Business and Microsoft Teams
Common	Office 365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints

In addition to basic internet services, there are third-party services that are only used to integrate functionality. While these are needed for integration, they're marked as optional in the Office 365 endpoints article, which means core functionality of the service will continue to function if the endpoint isn't accessible. Any network endpoint that is required will have the required attribute set to true. Any network endpoint that is optional will have the required attribute set to false and the notes attribute will detail the missing functionality you should expect if connectivity is blocked.

If you're trying to use Office 365 and are finding third-party services aren't accessible, you'll want to [ensure all FQDNs marked required or optional in this article are allowed through the proxy and firewall](#).

How do I block access to Microsoft's consumer services?

The tenant restrictions feature now supports blocking the use of all Microsoft consumer applications (MSA apps) such as OneDrive, Hotmail, and Xbox.com. This uses a separate header to the login.live.com endpoint. For more information, see [Use tenant restrictions to manage access to SaaS cloud applications](#).

My firewall requires IP Addresses and cannot process URLs. How do I configure it for Office 365?

Office 365 doesn't provide IP addresses of all required network endpoints. Some are provided as URLs only and are categorized as default. URLs in the default category that are required should be allowed through a proxy server. If you don't have a proxy server, look at how you have configured web requests for URLs that users type into the address bar of a web browser; the user doesn't provide an IP address either. The Office 365 default category URLs that do not provide IP addresses should be configured in the same way.

Related topics

[Office 365 IP Address and URL Web service](#)

[Microsoft Azure Datacenter IP Ranges](#)

[Microsoft Public IP Space](#)

[Network infrastructure requirements for Microsoft Intune](#)

[ExpressRoute and Power BI](#)

[Office 365 URLs and IP address ranges](#)

[Managing ExpressRoute for Office 365 connectivity](#)

[Office 365 Network Connectivity Principles](#)

Office 365 URLs and IP address ranges

10/28/2022 • 10 minutes to read • [Edit Online](#)

Office 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using Office 365 plans, including Government Community Cloud (GCC).

[Office 365 Worldwide \(+GCC\)](#) | [Office 365 operated by 21 Vianet](#) | [Office 365 U.S. Government DoD](#) | [Office 365 U.S. Government GCC High](#) |

NOTES	DOWNLOAD	USE
Last updated: 09/29/2022 -  Change Log subscription	Download: all required and optional destinations in one JSON formatted list.	Use: our proxy PAC files

Start with [Managing Office 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This cadence allows for customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Office 365. For detail on IP addresses used for network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections, see [Additional endpoints](#) for more information.

The endpoints are grouped into four service areas representing the three primary workloads and a set of common resources. The groups may be used to associate traffic flows with a particular application, however given that features often consume endpoints across multiple workloads, these groups can't effectively be used to restrict access.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as **Optimize**, **Allow**, or **Default**. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets that aren't required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.

You can read about these categories and guidance for their management in [New Office 365 endpoint categories](#).

- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Office 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute is not supported for this endpoint set.

Some routes may be advertised in more than one BGP community, making it possible for endpoints

within a given IP range to traverse the ER circuit, but still be unsupported. In all cases, the value of a given endpoint set's ER column should be respected. For more information about BGP communities, see [Using BGP communities in ExpressRoute for Office 365 scenarios](#).

- **Addresses:** Lists the FQDNs or wildcard domain names and IP address ranges for the endpoint set. Note that an IP address range is in CIDR format and may include many individual IP addresses in the specified network.
- **Ports:** Lists the TCP or UDP ports that are combined with listed IP addresses to form the network endpoint. You may notice some duplication in IP address ranges where there are different ports listed.

Exchange Online

ID	CATEGORY	ER	ADDRESSES	PORTS
1	Optimize Required	Yes	outlook.office.com, outlook.office365.com 13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22, 23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14, 131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22, 204.79.197.215/32, 2603:1006::/40, 2603:1016::/36, 2603:1026::/36, 2603:1036::/36, 2603:1046::/36, 2603:1056::/36, 2620:1ec:4::152/128, 2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128, 2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46, 2620:1ec:900::/46, 2620:1ec:a92::152/128, 2620:1ec:a92::153/128, 2a01:111:f400::/48	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
2	Allow Required	Yes	smtp.office365.com 13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22, 23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14, 131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22, 204.79.197.215/32, 2603:1006::/40, 2603:1016::/36, 2603:1026::/36, 2603:1036::/36, 2603:1046::/36, 2603:1056::/36, 2620:1ec:4::152/128, 2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128, 2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46, 2620:1ec:900::/46, 2620:1ec:a92::152/128, 2620:1ec:a92::153/128, 2a01:111:f400::/48	TCP: 587
5	Allow Optional Notes: Exchange Online IMAP4 migration	Yes	*.outlook.office.com, outlook.office365.com 13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22, 23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14, 131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22, 204.79.197.215/32, 2603:1006::/40, 2603:1016::/36, 2603:1026::/36, 2603:1036::/36, 2603:1046::/36, 2603:1056::/36, 2620:1ec:4::152/128, 2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128, 2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46, 2620:1ec:900::/46, 2620:1ec:a92::152/128, 2620:1ec:a92::153/128, 2a01:111:f400::/48	TCP: 143, 993

ID	CATEGORY	ER	ADDRESSES	PORTS
6	Allow Optional Notes: Exchange Online POP3 migration	Yes	*.outlook.office.com, outlook.office365.com 13.107.6.152/31, 13.107.18.10/31, 13.107.128.0/22, 23.103.160.0/20, 40.96.0.0/13, 40.104.0.0/15, 52.96.0.0/14, 131.253.33.215/32, 132.245.0.0/16, 150.171.32.0/22, 204.79.197.215/32, 2603:1006::/40, 2603:1016::/36, 2603:1026::/36, 2603:1036::/36, 2603:1046::/36, 2603:1056::/36, 2620:1ec:4::152/128, 2620:1ec:4::153/128, 2620:1ec:c::10/128, 2620:1ec:c::11/128, 2620:1ec:d::10/128, 2620:1ec:d::11/128, 2620:1ec:8f0::/46, 2620:1ec:900::/46, 2620:1ec:a92::152/128, 2620:1ec:a92::153/128, 2a01:111:f400::/48	TCP: 995
8	Default Required	No	*.outlook.com	TCP: 443, 80
9	Allow Required	Yes	*.protection.outlook.com 40.92.0.0/15, 40.107.0.0/16, 52.100.0.0/14, 52.238.78.88/32, 104.47.0.0/17, 2a01:111:f403::/48	TCP: 443
10	Allow Required	Yes	*.mail.protection.outlook.com 40.92.0.0/15, 40.107.0.0/16, 52.100.0.0/14, 104.47.0.0/17, 2a01:111:f400::/48, 2a01:111:f403::/48	TCP: 443, 25
154	Default Required	No	autodiscover. <tenant>.onmicrosoft.com	TCP: 443, 80

SharePoint Online and OneDrive for Business

ID	CATEGORY	ER	ADDRESSES	PORTS
31	Optimize Required	Yes	*.sharepoint.com 13.107.136.0/22, 40.108.128.0/17, 52.104.0.0/14, 104.146.128.0/17, 150.171.40.0/22, 2603:1061:1300::/40, 2620:1ec:8f8::/46, 2620:1ec:908::/46, 2a01:111:f402::/48	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
32	Default Optional Notes: OneDrive for Business: supportability, telemetry, APIs, and embedded email links	No	ssw.live.com, storage.live.com	TCP: 443
33	Default Optional Notes: SharePoint Hybrid Search - Endpoint to SearchContentService where the hybrid crawler feeds documents	No	*.search.production.apicentral.trafficmanager.net, *.search.production.emea.trafficmanager.net, *.search.production.us.trafficmanager.net	TCP: 443
35	Default Required	No	*.wns.windows.com, admin.onedrive.com, officeclient.microsoft.com	TCP: 443, 80
36	Default Required	No	g.live.com, oneclient.sfx.ms	TCP: 443, 80
37	Default Required	No	*.sharepointonline.com spoprod-a.akamaihd.net	TCP: 443, 80
39	Default Required	No	*.svc.ms	TCP: 443, 80

Skype for Business Online and Microsoft Teams

ID	CATEGORY	ER	ADDRESSES	PORTS
11	Optimize Required	Yes	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 2603:1063::/38	UDP: 3478, 3479, 3480, 3481
12	Allow Required	Yes	*.lync.com, *.teams.microsoft.com, teams.microsoft.com 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2603:1063::/38, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
13	Allow Required	Yes	*.broadcast.skype.com, broadcast.skype.com 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2603:1063::/38, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443
15	Default Required	No	*.sfbassets.com	TCP: 443, 80
16	Default Required	No	*.keydelivery.mediaservice.windows.net, *.streaming.mediaservices.windows.net, mlccdn.blob.core.windows.net	TCP: 443
17	Default Required	No	aka.ms	TCP: 443
18	Default Optional Notes: Federation with Skype and public IM connectivity: Contact picture retrieval	No	*.users.storage.live.com	TCP: 443
19	Default Optional Notes: Applies only to those who deploy the Conference Room Systems	No	*.adl.windows.com	TCP: 443, 80
22	Allow Optional Notes: Teams: Messaging interop with Skype for Business	Yes	*.skypeforbusiness.com 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2603:1063::/38, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443
27	Default Required	No	*.mstea.ms, *.secure.skypeassets.com, mlccdnprod.azureedge.net	TCP: 443
127	Default Required	No	*.skype.com	TCP: 443, 80
167	Default Required	No	*.ecdn.microsoft.com	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
180	Default Required	No	compass-ssl.microsoft.com	TCP: 443

Microsoft 365 Common and Office Online

ID	CATEGORY	ER	ADDRESSES	PORTS
41	Default Optional Notes: Microsoft Stream	No	*.microsoftstream.com	TCP: 443
43	Default Optional Notes: Microsoft Stream 3rd party integration (including CDNs)	No	nps.onyx.azure.net	TCP: 443
44	Default Optional Notes: Microsoft Stream - unauthenticated	No	*.azureedge.net, *.media.azure.net, *.streaming.mediaservices.windows.net	TCP: 443
45	Default Optional Notes: Microsoft Stream	No	*.keydelivery.mediaservices.windows.net	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
46	Allow Required	Yes	*.officeapps.live.com, *.online.office.com, office.live.com 13.107.6.171/32, 13.107.18.15/32, 13.107.140.6/32, 52.108.0.0/14, 52.238.106.116/32, 52.244.37.168/32, 52.244.203.72/32, 52.244.207.172/32, 52.244.223.198/32, 52.247.150.191/32, 2603:1010:2::cb/128, 2603:1010:200::c7/128, 2603:1020:200::682f:a0fd/128, 2603:1020:201:9::c6/128, 2603:1020:600::a1/128, 2603:1020:700::a2/128, 2603:1020:800:2::6/128, 2603:1020:900::8/128, 2603:1030:7::749/128, 2603:1030:800:5::bfee:ad3c/128, 2603:1030:f00::17/128, 2603:1030:1000::21a/128, 2603:1040:200::4f3/128, 2603:1040:401::762/128, 2603:1040:601::60f/128, 2603:1040:a01::1e/128, 2603:1040:c01::28/128, 2603:1040:e00:1::2f/128, 2603:1040:f00::1f/128, 2603:1050:1::cd/128, 2620:1ec:c::15/128, 2620:1ec:8fc::6/128, 2620:1ec:a92::171/128, 2a01:111:f100:2000::a83e:3019/128, 2a01:111:f100:2002::8975:2d79/128, 2a01:111:f100:2002::8975:2da8/128, 2a01:111:f100:7000::6fdd:6cd5/128, 2a01:111:f100:a004::bfeb:88cf/128	TCP: 443, 80
47	Default Required	No	*.office.net	TCP: 443, 80
49	Default Required	No	*.onenote.com	TCP: 443
50	Default Optional Notes: OneNote notebooks (wildcards)	No	*.microsoft.com	TCP: 443
51	Default Required	No	*cdn.onenote.net	TCP: 443
53	Default Required	No	ajax.aspnetcdn.com, apis.live.net, officeapps.live.com, www.onedrive.com	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
56	Allow Required	Yes	*.auth.microsoft.com, *.microsoft.com, *.msidentity.com, *.msidentity.com, account.activedirectory.windowsazure.com, accounts.accesscontrol.windows.net, adminwebservice.microsoftonline.com, api.passwordreset.microsoftonline.com, autologon.microsoftazuread-sso.com, becws.microsoftonline.com, ccs.login.microsoftonline.com, clientconfig.microsoftonline-p.net, companymanager.microsoftonline.com, device.login.microsoftonline.com, graph.microsoft.com, graph.windows.net, login.microsoft.com, login.microsoftonline.com, login.microsoftonline-p.com, login.windows.net, logincert.microsoftonline.com, loginex.microsoftonline.com, login-us.microsoftonline.com, nexus.microsoftonline-p.com, passwordreset.microsoftonline.com, provisioningapi.microsoftonline.com 20.190.128.0/18, 40.126.0.0/18, 2603:1006:2000::/48, 2603:1007:2000::/48, 2603:1016:1400::/48, 2603:1017::/48, 2603:1026:3000::/48, 2603:1027:1::/48, 2603:1036:3000::/48, 2603:1037:1::/48, 2603:1046:2000::/48, 2603:1047:1::/48, 2603:1056:2000::/48, 2603:1057:2::/48	TCP: 443, 80
59	Default Required	No	*.hip.live.com, *.microsoftonline.com, *.microsoftonline-p.com, *.msauth.net, *.msauthimages.net, *.msecnd.net, *.msftauth.net, *.msftauthimages.net, *.phonefactor.net, enterpriseregistration.windows.net, management.azure.com, policykeyservice.dc.ad.msft.net	TCP: 443, 80
64	Allow Required	Yes	*.compliance.microsoft.com, *.protection.office.com, *.security.microsoft.com, compliance.microsoft.com, defender.microsoft.com, protection.office.com, security.microsoft.com 52.108.0.0/14, 2603:1006:1400::/40, 2603:1016:2400::/40, 2603:1026:2400::/40, 2603:1036:2400::/40, 2603:1046:1400::/40, 2603:1056:1400::/40, 2a01:111:200a:a::/64, 2a01:111:2035:8::/64, 2a01:111:f406:1::/64, 2a01:111:f406:c00::/64, 2a01:111:f406:1004::/64, 2a01:111:f406:1805::/64, 2a01:111:f406:3404::/64, 2a01:111:f406:8000::/64, 2a01:111:f406:8801::/64, 2a01:111:f406:a003::/64	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
65	Allow Required	Yes	account.office.net 52.108.0.0/14, 2603:1006:1400::/40, 2603:1016:2400::/40, 2603:1026:2400::/40, 2603:1036:2400::/40, 2603:1046:1400::/40, 2603:1056:1400::/40, 2a01:111:200a:a::/64, 2a01:111:2035:8::/64, 2a01:111:f406:1::/64, 2a01:111:f406:c00::/64, 2a01:111:f406:1004::/64, 2a01:111:f406:1805::/64, 2a01:111:f406:3404::/64, 2a01:111:f406:8000::/64, 2a01:111:f406:8801::/64, 2a01:111:f406:a003::/64	TCP: 443, 80
66	Default Required	No	*.portal.cloudappsecurity.com	TCP: 443
67	Default Optional Notes: Security and Compliance Center eDiscovery export	No	*.blob.core.windows.net	TCP: 443
68	Default Optional Notes: Portal and shared: 3rd party office integration. (including CDNs)	No	firstpartyapps.oaspapps.com, prod.firstpartyapps.oaspapps.com.akadns.net, telemetryservice.firstpartyapps.oaspapps.com, wus-firstpartyapps.oaspapps.com	TCP: 443
69	Default Required	No	*.aria.microsoft.com, *.events.data.microsoft.com	TCP: 443
70	Default Required	No	*.o365weve.com, amp.azure.net, appsforoffice.microsoft.com, assets.onestore.ms, auth.gfx.ms, c1.microsoft.com, dgps.support.microsoft.com, docs.microsoft.com, msdn.microsoft.com, platform.linkedin.com, prod.msocdn.com, shellprod.msocdn.com, support.microsoft.com, technet.microsoft.com	TCP: 443
71	Default Required	No	*.office365.com	TCP: 443, 80
72	Default Optional Notes: Azure Rights Management (RMS) with Office 2010 clients	No	*.cloudapp.net	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
73	Default Required	No	*.aadrm.com, *.azurerms.com, *.informationprotection.azure.com, ecn.dev.virtualearth.net, informationprotection.hosting.portal.azure.net	TCP: 443
75	Default Optional Notes: Graph.windows.net, Office 365 Management Pack for Operations Manager, SecureScore, Azure AD Device Registration, Forms, StaffHub, Application Insights, captcha services	No	*.sharepointonline.com dc.services.visualstudio.com, mem.gfx.ms, staffhub.ms	TCP: 443
78	Default Optional Notes: Some Office 365 features require endpoints within these domains (including CDNs). Many specific FQDNs within these wildcards have been published recently as we work to either remove or better explain our guidance relating to these wildcards.	No	*.microsoft.com, *.msocdn.com, *.onmicrosoft.com	TCP: 443, 80
79	Default Required	No	o15.officeredir.microsoft.com, officepreviewredir.microsoft.com, officeredir.microsoft.com, r.office.microsoft.com	TCP: 443, 80
83	Default Required	No	activation.sls.microsoft.com	TCP: 443
84	Default Required	No	cr1.microsoft.com	TCP: 443, 80
86	Default Required	No	office15client.microsoft.com, officeclient.microsoft.com	TCP: 443
89	Default Required	No	go.microsoft.com	TCP: 443, 80
91	Default Required	No	ajax.aspnetcdn.com, cdn.odc.officeapps.live.com	TCP: 443, 80
92	Default Required	No	officecdn.microsoft.com, officecdn.microsoft.com.edgesuite.net	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
93	Default Optional Notes: ProPlus: auxiliary URLs	No	*.virtualearth.net, c. excelbingmap.firstpartyapps.oaspapps.com, ocos-office365-s2s.msedge.net, peoplegraph.firstpartyapps.oaspapps.com, tse1.mm.bing.net, wikipedia.firstpartyapps.oaspapps.com, www.bing.com	TCP: 443, 80
95	Default Optional Notes: Outlook for Android and iOS	No	*.acompli.net, *.outlookmobile.com	TCP: 443
96	Default Optional Notes: Outlook for Android and iOS: Authentication	No	login.windows- ppe.net	TCP: 443
97	Default Optional Notes: Outlook for Android and iOS: Consumer Outlook.com and OneDrive integration	No	account.live.com, login.live.com	TCP: 443
105	Default Optional Notes: Outlook for Android and iOS: Outlook Privacy	No	www.acompli.com	TCP: 443
114	Default Optional Notes: Office Mobile URLs	No	*.appex.bing.com, *.ap rf.msn.com, c.bing.com, c.live.com, d.docs.live.net, directory.services.live.com, docs.live.net, partnerservices.getmicrosoftkey.com, signup.live.com	TCP: 443, 80
116	Default Optional Notes: Office for iPad URLs	No	account.live.com, auth.gfx.ms, login.live.com	TCP: 443, 80
117	Default Optional Notes: Yammer	No	*.yammer.com, *.yammerusercontent.com	TCP: 443
118	Default Optional Notes: Yammer CDN	No	*.assets- yammer.com	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
121	Default Optional Notes: Planner: auxiliary URLs	No	www.outlook.com	TCP: 443, 80
122	Default Optional Notes: Sway CDNs	No	eus-www.sway-cdn.com, eus-www.sway-extensions.com, wus-www.sway-cdn.com, wus-www.sway-extensions.com	TCP: 443
124	Default Optional Notes: Sway	No	sway.com, www.sway.com	TCP: 443
125	Default Required	No	*.entrust.net, *.geotrust.com, *.omniroot.com, *.public-trust.com, *.symcb.com, *.symcd.com, *.verisign.com, *.verisign.net, apps.identrust.com, cacerts.digicert.com, cert.int-x3.letsencrypt.org, crl.globalsign.com, crl.globalsign.net, crl.identrust.com, crl3.digicert.com, crl4.digicert.com, isrg.trustid.ocsp.identrust.com, mscrl.microsoft.com, ocsp.digicert.com, ocsp.globalsign.com, ocsp.msocsp.com, ocsp2.globalsign.com, ocsp.x.digicert.com, secure.globalsign.com, www.digicert.com, www.microsoft.com	TCP: 443, 80
126	Default Optional Notes: Connection to the speech service is required for Office Dictation features. If connectivity is not allowed, Dictation will be disabled.	No	officespeech.platform.microsoft.com	TCP: 443
128	Default Required	No	*.manage.microsoft.com	TCP: 443
147	Default Required	No	*.office.com	TCP: 443, 80
148	Default Required	No	cdnprod.myanalytics.microsoft.com, myanalytics.microsoft.com, myanalytics-gcc.microsoft.com	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
152	Default Optional Notes: These endpoints enables the Office Scripts functionality in Office clients available through the Automate tab. This feature can also be disabled through the Office 365 Admin portal.	No	*.microsoftusercontent.com	TCP: 443
153	Default Required	No	*.azure-apim.net, *.flow.microsoft.com, *.powerapps.com	TCP: 443
156	Default Required	No	*.activity.windows.com activity.windows.com	TCP: 443
157	Default Required	No	ocsp.int-x3.letsencrypt.org	TCP: 80
158	Default Required	No	*.cortana.ai	TCP: 443
159	Default Required	No	admin.microsoft.com	TCP: 443, 80
160	Default Required	No	cdn.odc.officeapps.live.com cdn.uci.officeapps.live.com	TCP: 443, 80

NOTE

For recommendations on Yammer IP addresses and URLs, see [Using hard-coded IP addresses for Yammer is not recommended](#) on the Yammer blog.

Related Topics

[Additional endpoints not included in the Office 365 IP Address and URL Web service](#)

[Managing Office 365 endpoints](#)

[General Microsoft Stream endpoints](#)

[Monitor Microsoft 365 connectivity](#)

[Root CA and the Intermediate CA bundle on the third-party application system](#)

[Client connectivity](#)

[Content delivery networks](#)

[Microsoft Azure IP Ranges and Service Tags – Public Cloud](#)

[Microsoft Azure IP Ranges and Service Tags – US Government Cloud](#)

[Microsoft Azure IP Ranges and Service Tags – China Cloud](#)

[Microsoft Public IP Space](#)

[Service Name and Transport Protocol Port Number Registry](#)

Office 365 U.S. Government DoD endpoints

10/28/2022 • 5 minutes to read • [Edit Online](#)

Applies To: Office 365 Admin

Office 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using Office 365 U.S. Government DoD plans only.

Office 365 endpoints: [Worldwide \(including GCC\)](#) | [Office 365 operated by 21 Vianet](#) | [Office 365 U.S. Government DoD](#) | [Office 365 U.S. Government GCC High](#)

NOTES	DOWNLOAD
Last updated: 09/29/2022 -  Change Log subscription	Download: the full list in JSON format

Start with [Managing Office 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This lets customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Office 365. It doesn't include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections. For more information, see [Additional endpoints not included in the web service](#).

The endpoints are grouped into four service areas. The first three service areas can be independently selected for connectivity. The fourth service area is a common dependency (called Microsoft 365 Common and Office) and must always have network connectivity.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as "Optimize", "Allow", or "Default". You can read about these categories and guidance for management of them at <https://aka.ms/pnc>. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets that aren't required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.
- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Office 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute is not supported for this endpoint set. However, it should not be assumed that no routes are advertised for an endpoint set where ER is **No**. If you plan to use Azure AD Connect, read the [special considerations section](#) to ensure you have the appropriate Azure AD Connect

configuration.

- **Addresses:** Lists the FQDNs or wildcard domain names and IP Address ranges for the endpoint set. Note that an IP Address range is in CIDR format and may include many individual IP Addresses in the specified network.
- **Ports:** Lists the TCP or UDP ports that are combined with the Addresses to form the network endpoint. You may notice some duplication in IP Address ranges where there are different ports listed.

Exchange Online

ID	CATEGORY	ER	ADDRESSES	PORTS
1	Optimize Required	Yes	outlook- dod.office365.us, webmail.apps.mil 20.35.192.0/20, 40.66.24.0/21, 131.253.80.0/24, 131.253.83.64/26, 131.253.84.0/26, 131.253.84.128/26, 131.253.87.0/25, 131.253.87.128/28, 131.253.87.160/27, 131.253.87.192/28, 131.253.87.224/28, 131.253.88.16/28, 131.253.88.64/28, 131.253.88.80/28, 131.253.88.112/28, 131.253.88.176/28, 131.253.88.208/28, 131.253.88.224/28, 2001:489a:2200:2c::/62, 2001:489a:2200:38::/62, 2001:489a:2200:40::/62, 2001:489a:2200:68::/61, 2001:489a:2200:70::/61, 2001:489a:2200:78::/64, 2001:489a:2200:7a::/63, 2001:489a:2200:7c::/64, 2001:489a:2200:7e::/64, 2001:489a:2200:81::/64, 2001:489a:2200:84::/63, 2001:489a:2200:87::/64, 2001:489a:2200:8b::/64, 2001:489a:2200:8d::/64, 2001:489a:2200:8e::/64, 2001:489a:2200:500::/56, 2001:489a:2200:700::/56	TCP: 443, 80
4	Default Required	Yes	outlook- dod.office365.us, webmail.apps.mil	TCP: 143, 25, 587, 993, 995
5	Default Required	Yes	attachments-dod.office365.us, net.us, autodiscover. <tenant>.mail.onmicrosoft.com, autodiscover. <tenant>.mail.onmicrosoft.us, autodiscover. <tenant>.onmicrosoft.com, autodiscover. <tenant>.onmicrosoft.us, autodiscover-s- dod.office365.us	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
6	Allow Required	Yes	*.protection.apps.mil, *.protection.office365.us 23.103.191.0/24, 23.103.199.0/25, 23.103.204.0/22, 52.181.167.52/32, 52.181.167.91/32, 52.182.95.219/32, 2001:489a:2202::/62, 2001:489a:2202:8::/62, 2001:489a:2202:2000::/63	TCP: 25, 443

SharePoint Online and OneDrive for Business

ID	CATEGORY	ER	ADDRESSES	PORTS
9	Optimize Required	Yes	*.dps.mil, *.sharepoint-mil.us 20.34.12.0/22, 104.212.48.0/23, 2001:489a:2204::/63, 2001:489a:2204:c00::/54	TCP: 443, 80
10	Default Required	No	*.wns.windows.com, g.live.com, oneclient.sfx.ms	TCP: 443, 80
19	Allow Required	Yes	*.od.apps.mil, od.apps.mil	TCP: 443, 80
20	Default Required	No	*.svc.ms, az741266.vo.msecnd.net, spoprod-a.akamaihd.net, static.sharepointonline.com	TCP: 443, 80

Skype for Business Online and Microsoft Teams

ID	CATEGORY	ER	ADDRESSES	PORTS
7	Optimize Required	Yes	*.dod.teams.microsoft. *.online.dod.skypeforbusiness. dod.teams.microsoft.us 52.127.64.0/21, 52.180.249.148/32, 52.180.252.118/32, 52.180.252.187/32, 52.180.253.137/32, 52.180.253.154/32, 52.181.165.243/32, 52.181.166.119/32, 52.181.167.43/32, 52.181.167.64/32, 52.181.200.104/32, 104.212.32.0/22, 104.212.60.0/23, 195.134.240.0/22	TCP: 443 UDP: 3478, 3479, 3480, 3481
21	Default Required	No	dodteamsapiwebcontent. msteamsstatics.blob.core.usgovcloudapi.net, statics.teams.microsoft.com	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
22	Allow Required	Yes	endpoint1-proddodcecomp dodc.streaming.media.usgovcloudapi.net, endpoint1-proddodeacompsvc- dode.streaming.media.usgovcloudapi.net 52.181.167.113/32, 52.182.52.226/32	TCP: 443

Microsoft 365 Common and Office Online

ID	CATEGORY	ER	ADDRESSES	PORTS
11	Allow Required	Yes	*.dod.online.office365 52.127.80.0/23, 52.181.164.39/32, 52.182.95.191/32	TCP: 443
12	Default Required	No	*.office365.us	TCP: 443, 80
13	Allow Required	Yes	*.auth.microsoft.us, *.gov.us.microsoftonline.com, dod-graph.microsoft.us, graph.microsoftazure.us, login.microsoftonline.us 20.140.232.0/23, 52.126.194.0/23, 2001:489a:3500::/50	TCP: 443
14	Default Required	No	*.msauth.net, *.msauthimages.us, *.msftauth.net, *.msftauthimages.us, clientconfig.microsoftonline- p.net, graph.windows.net, login.microsoftonline.com, login.microsoftonline-p.com, login.windows.net, loginex.microsoftonline.com, login-us.microsoftonline.com, mscr1.microsoft.com, nexus.microsoftonline-p.com, secure.aadcdn.microsoftonline- p.com	TCP: 443
15	Allow Required	Yes	portal.apps.mil, reports.apps.mil, webshell.dodsuite.office365.us, www.ohome.apps.mil 52.127.72.42/32, 52.127.76.42/32, 52.180.251.166/32, 52.181.24.112/32, 52.181.160.19/32, 52.181.160.113/32, 52.181.160.236/32, 52.182.24.200/32, 52.182.54.237/32, 52.182.92.132/32	TCP: 443
16	Allow Required	Yes	*.osi.apps.mil, dod.loki.office365.us 52.127.72.0/21, 2001:489a:2206::/48	TCP: 443

ID	CATEGORY	ER	ADDRESSES	PORTS
17	Default Required	No	activation.sls.microsoft.com, crl.microsoft.com, go.microsoft.com, insertmedia.bing.office.net, ocsa.officeapps.live.com, ocsredirect.officeapps.live.com, ocws.officeapps.live.com, office15client.microsoft.com, officecdn.microsoft.com, officecdn.microsoft.com.edgesuite.net, officepreviewredirect.microsoft.com, officeredir.microsoft.com, ols.officeapps.live.com, r.office.microsoft.com	TCP: 443, 80
18	Default Required	No	cdn.odc.officeapps.live.com, odc.officeapps.live.com, officeclient.microsoft.com	TCP: 443, 80
24	Default Required	No	lpcres.delve.office.com	TCP: 443
25	Default Required	No	*.cdn.office.net	TCP: 443
26	Allow Required	Yes	*.compliance.apps.mil, *.security.apps.mil, compliance.apps.mil, security.apps.mil 23.103.191.0/24, 23.103.199.0/25, 23.103.204.0/22, 52.181.167.52/32, 52.181.167.91/32, 52.182.95.219/32, 2001:489a:2202::/62, 2001:489a:2202:8::/62, 2001:489a:2202:2000::/63	TCP: 443, 80
28	Default Required	No	activity.windows.com, dod.activity.windows.us	TCP: 443
29	Default Required	No	dod-mtis.cortana.ai	TCP: 443
30	Default Required	No	*.aadrm.us, *.informationprotection.azure.us	TCP: 443
31	Default Required	No	pf.events.data.microsoft.com, pf.pipe.aria.microsoft.com	TCP: 443, 80
32	Default Required	No	config.apps.mil	TCP: 443

Notes for this table:

- The Security and Compliance Center (SCC) provides support for Azure ExpressRoute for Office 365. The same applies for many features exposed through the SCC such as Reporting, Auditing, eDiscovery (Premium), Unified DLP, and Data Governance. Two specific features, PST Import and eDiscovery Export, currently do not support Azure ExpressRoute with only Office 365 route filters due to their dependency on Azure Blob Storage. To consume those features, you need separate connectivity to Azure Blob Storage using any supportable Azure connectivity options, which include Internet connectivity or Azure ExpressRoute with Azure Public route filters. You have to evaluate establishing such connectivity for both of those features. The Office 365 Information Protection team is aware of this limitation and is actively

working to bring support for Azure ExpressRoute for Office 365 as limited to Office 365 route filters for both of those features.

- There are additional optional endpoints for Microsoft 365 Apps for enterprise that are not listed and are not required for users to launch Microsoft 365 Apps for enterprise applications and edit documents. Optional endpoints are hosted in Microsoft datacenters and do not process, transmit, or store customer data. We recommend that user connections to these endpoints be directed to the default Internet egress perimeter.

Office 365 U.S. Government GCC High endpoints

10/28/2022 • 5 minutes to read • [Edit Online](#)

Applies To: Office 365 Admin

Office 365 requires connectivity to the Internet. The endpoints below should be reachable for customers using Office 365 U.S. Government GCC High plans only.

Office 365 endpoints: [Worldwide \(including GCC\)](#) | [Office 365 operated by 21 Vianet](#) | [Office 365 U.S. Government DoD](#) | [Office 365 U.S. Government GCC High](#)

NOTES	DOWNLOAD
Last updated: 09/29/2022 -  Change Log subscription	Download: the full list in JSON format

Start with [Managing Office 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This lets customers who don't yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you're using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Office 365. It does not include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections.

The endpoints are grouped into four service areas. The first three service areas can be independently selected for connectivity. The fourth service area is a common dependency (called Microsoft 365 Common and Office) and must always have network connectivity.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as "Optimize", "Allow", or "Default". You can read about these categories and guidance for management of them at <https://aka.ms/pnc>. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets which are not required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you're excluding an entire service area, the endpoint sets listed as required don't require connectivity.
- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Office 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute is not supported for this endpoint set. However, it should not be assumed that no routes are advertised for an endpoint set where ER is **No**. If you plan to use Azure AD Connect, read the [special considerations section](#) to ensure you have the appropriate Azure AD Connect

configuration.

- **Addresses:** Lists the FQDNs or wildcard domain names and IP Address ranges for the endpoint set. Note that an IP Address range is in CIDR format and may include many individual IP Addresses in the specified network.
- **Ports:** Lists the TCP or UDP ports that are combined with the Addresses to form the network endpoint. You may notice some duplication in IP Address ranges where there are different ports listed.

Exchange Online

ID	CATEGORY	ER	ADDRESSES	PORTS
1	Optimize Required	Yes	outlook.office365.us 20.35.208.0/20, 20.35.240.0/21, 40.66.16.0/21, 131.253.83.0/26, 131.253.84.64/26, 131.253.84.192/26, 131.253.86.0/24, 131.253.87.144/28, 131.253.87.208/28, 131.253.87.240/28, 131.253.88.0/28, 131.253.88.32/28, 131.253.88.48/28, 131.253.88.96/28, 131.253.88.128/28, 131.253.88.144/28, 131.253.88.160/28, 131.253.88.192/28, 131.253.88.240/28, 2001:489a:2200:28::/62, 2001:489a:2200:3c::/62, 2001:489a:2200:44::/62, 2001:489a:2200:58::/61, 2001:489a:2200:60::/62, 2001:489a:2200:79::/64, 2001:489a:2200:7d::/64, 2001:489a:2200:7f::/64, 2001:489a:2200:80::/64, 2001:489a:2200:82::/63, 2001:489a:2200:86::/64, 2001:489a:2200:88::/63, 2001:489a:2200:8a::/64, 2001:489a:2200:8c::/64, 2001:489a:2200:8f::/64, 2001:489a:2200:100::/56, 2001:489a:2200:400::/56, 2001:489a:2200:600::/56	TCP: 443, 80
4	Default Required	Yes	attachments.office365-us-1443.us autodiscover. <tenant>.mail.onmicrosoft.com, autodiscover. <tenant>.mail.onmicrosoft.us, autodiscover. <tenant>.onmicrosoft.com, autodiscover. <tenant>.onmicrosoft.us, autodiscover-s.office365.us	TCP: 443, 80
5	Default Required	Yes	outlook.office365.us	TCP: 143, 25, 587, 993, 995

ID	CATEGORY	ER	ADDRESSES	PORTS
6	Allow Required	Yes	*.manage.office365.us, TCP: 25, 443 *.protection.office365.us, *.scc.office365.us, manage.office365.us, scc.office365.us 13.72.179.197/32, 13.72.183.70/32, 23.103.191.0/24, 23.103.199.128/25, 23.103.208.0/22, 52.227.170.14/32, 52.227.170.120/32, 52.227.178.94/32, 52.227.180.138/32, 52.227.182.149/32, 52.238.74.212/32, 52.244.65.13/32, 2001:489a:2202:4::/62, 2001:489a:2202:c::/62, 2001:489a:2202:2000::/63	

SharePoint Online and OneDrive for Business

ID	CATEGORY	ER	ADDRESSES	PORTS
9	Optimize Required	Yes	*.sharepoint.us 20.34.8.0/22, 104.212.50.0/23, 2001:489a:2204:2::/63, 2001:489a:2204:800::/54	TCP: 443, 80
10	Default Required	No	*.wns.windows.com, admin.onedrive.us, g.live.com, oneclient.sfx.ms	TCP: 443, 80
20	Default Required	No	*.svc.ms, az741266.vo.msecnd.net, spoprod-a.akamaihd.net, static.sharepointonline.com	TCP: 443, 80

Skype for Business Online and Microsoft Teams

ID	CATEGORY	ER	ADDRESSES	PORTS
7	Optimize Required	Yes	52.127.88.0/21, 104.212.44.0/22, 195.134.228.0/22	UDP: 3478, 3479, 3480, 3481
21	Default Required	No	msteamsstatics.blob.core.usgovcloudapi.net, statics.teams.microsoft.com, teamsapiwebcontent.blob.core.usgovcloudapi.net	TCP: 443
31	Allow Required	Yes	*.gov.skypeforbusiness, TCP: 443, 80 *.gov.teams.microsoft.us, gov.teams.microsoft.us 52.127.88.0/21, 104.212.44.0/22, 195.134.228.0/22	

Microsoft 365 Common and Office Online

ID	CATEGORY	ER	ADDRESSES	PORTS
11	Allow Required	Yes	*.gov.office365.us 52.127.37.0/24, 52.127.82.0/23	TCP: 443
12	Default Required	Yes	*.cdn.office365.us	TCP: 443
13	Allow Required	Yes	*.auth.microsoft.us, *.gov.us.microsoftonline.com, graph.microsoft.us, graph.microsoftazure.us, login.microsoftonline.us 20.140.232.0/23, 52.126.194.0/23, 2001:489a:3500::/50	TCP: 443
14	Default Required	No	*.msauth.net, *.msauthimages.us, *.msftauth.net, *.msftauthimages.us, clientconfig.microsoftonline- p.net, graph.windows.net, login.microsoftonline.com, login.microsoftonline-p.com, login.windows.net, loginex.microsoftonline.com, login-us.microsoftonline.com, mscrl.microsoft.com, nexus.microsoftonline-p.com, secure.aadcdn.microsoftonline- p.com	TCP: 443
15	Default Required	No	officehome.msocdn.us, prod.msocdn.us	TCP: 443, 80
16	Allow Required	Yes	portal.office365.us, www.office365.us 13.72.179.48/32, 52.227.167.206/32, 52.227.170.242/32	TCP: 443, 80
17	Allow Required	Yes	*.osi.office365.us, gcchigh.loki.office365.us, tasks.office365.us 52.127.240.0/20, 2001:489a:2206::/48	TCP: 443
18	Default Required	No	activation.sls.microsoft.com, crl.microsoft.com, go.microsoft.com, insertmedia.bing.office.net, ocsa.officeapps.live.com, ocsredirect.officeapps.live.com, ocws.officeapps.live.com, office15client.microsoft.com, officecdn.microsoft.com, officecdn.microsoft.com.edgesuite.net, officepreviewredirect.microsoft.com, officeredir.microsoft.com, ols.officeapps.live.com, r.office.microsoft.com	TCP: 443, 80
19	Default Required	No	cdn.odc.officeapps.live.com, odc.officeapps.live.com, officeclient.microsoft.com	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
23	Default Required	No	*.office365.us	TCP: 443, 80
24	Default Required	No	lpcres.delve.office.com	TCP: 443
25	Default Required	No	*.cdn.office.net	TCP: 443
26	Allow Required	Yes	*.compliance.microsoft.com, *.security.microsoft.us, compliance.microsoft.us, security.microsoft.us 13.72.179.197/32, 13.72.183.70/32, 23.103.191.0/24, 23.103.199.128/25, 23.103.208.0/22, 52.227.170.14/32, 52.227.170.120/32, 52.227.178.94/32, 52.227.180.138/32, 52.227.182.149/32, 52.238.74.212/32, 52.244.65.13/32, 2001:489a:2202:4::/62, 2001:489a:2202:c::/62, 2001:489a:2202:2000::/63	TCP: 443, 80
28	Default Required	No	activity.windows.com, gcc- high.activity.windows.us	TCP: 443
29	Default Required	No	gcch- mtis.cortana.ai	TCP: 443
30	Default Required	No	*.aadrm.us, *.informationprotection.azure.us	TCP: 443
32	Default Required	No	tb.events.data.microsoft.com, tb.pipe.aria.microsoft.com	TCP: 443, 80

Notes for this table:

- The Security and Compliance Center (SCC) provides support for Azure ExpressRoute for Office 365. The same applies for many features exposed through the SCC such as Reporting, Auditing, eDiscovery (Premium), Unified DLP, and Data Governance. Two specific features, PST Import and eDiscovery Export, currently don't support Azure ExpressRoute with only Office 365 route filters due to their dependency on Azure Blob Storage. To consume those features, you need separate connectivity to Azure Blob Storage using any supportable Azure connectivity options, which include Internet connectivity or Azure ExpressRoute with Azure Public route filters. You have to evaluate establishing such connectivity for both of those features. The Office 365 Information Protection team is aware of this limitation and is actively working to bring support for Azure ExpressRoute for Office 365 as limited to Office 365 route filters for both of those features.
- There are additional optional endpoints for Microsoft 365 Apps for enterprise that are not listed and are not required for users to launch Microsoft 365 Apps for enterprise applications and edit documents. Optional endpoints are hosted in Microsoft data centers and don't process, transmit, or store customer data. We recommend that user connections to these endpoints be directed to the default Internet egress perimeter.

URLs and IP address ranges for Office 365 operated by 21Vianet

10/28/2022 • 4 minutes to read • [Edit Online](#)

Applies To: Office 365 operated by 21Vianet - Small Business Admin, Office 365 operated by 21Vianet - Admin

Summary: The following endpoints (FQDNs, ports, URLs, IPv4, and IPv6 prefixes) apply to Office 365 operated by 21 Vianet and are designed to deliver productivity services to organizations using only these plans.

Office 365 endpoints: [Worldwide \(including GCC\)](#) | [Office 365 operated by 21 Vianet](#) | [Office 365 U.S. Government DoD](#) | [Office 365 U.S. Government GCC High](#) |

Last updated: 07/28/2022 -  [Change Log subscription](#)

Download: all required and optional destinations in one [JSON formatted](#) list.

Start with [Managing Office 365 endpoints](#) to understand our recommendations for managing network connectivity using this data. Endpoints data is updated as needed at the beginning of each month with new IP Addresses and URLs published 30 days in advance of being active. This allows for customers who do not yet have automated updates to complete their processes before new connectivity is required. Endpoints may also be updated during the month if needed to address support escalations, security incidents, or other immediate operational requirements. The data shown on this page below is all generated from the REST-based web services. If you are using a script or a network device to access this data, you should go to the [Web service](#) directly.

Endpoint data below lists requirements for connectivity from a user's machine to Office 365. It does not include network connections from Microsoft into a customer network, sometimes called hybrid or inbound network connections.

The endpoints are grouped into four service areas. The first three service areas can be independently selected for connectivity. The fourth service area is a common dependency (called Microsoft 365 Common and Office) and must always have network connectivity.

Data columns shown are:

- **ID:** The ID number of the row, also known as an endpoint set. This ID is the same as is returned by the web service for the endpoint set.
- **Category:** Shows whether the endpoint set is categorized as "Optimize", "Allow", or "Default". You can read about these categories and guidance for management of them at <https://aka.ms/pnc>. This column also lists which endpoint sets are required to have network connectivity. For endpoint sets which are not required to have network connectivity, we provide notes in this field to indicate what functionality would be missing if the endpoint set is blocked. If you are excluding an entire service area, the endpoint sets listed as required do not require connectivity.
- **ER:** This is **Yes** if the endpoint set is supported over Azure ExpressRoute with Office 365 route prefixes. The BGP community that includes the route prefixes shown aligns with the service area listed. When ER is **No**, this means that ExpressRoute is not supported for this endpoint set. However, it should not be assumed that no routes are advertised for an endpoint set where ER is **No**.
- **Addresses:** Lists the FQDNs or wildcard domain names and IP Address ranges for the endpoint set. Note that an IP Address range is in CIDR format and may include many individual IP Addresses in the specified network.

- **Ports:** Lists the TCP or UDP ports that are combined with the Addresses to form the network endpoint.
You may notice some duplication in IP Address ranges where there are different ports listed.

Exchange Online

ID	CATEGORY	ER	ADDRESSES	PORTS
1	Optimize Required	No	*.partner.outlook.cn 40.73.132.0/24, 40.73.164.128/25, 40.73.165.0/26, 42.159.40.0/24, 42.159.44.0/22, 42.159.163.128/25, 42.159.165.0/24, 42.159.172.0/22	TCP: 443, 80
2	Allow Required	No	42.159.33.192/27, 42.159.36.0/24, 42.159.161.192/27, 42.159.164.0/24, 139.219.16.0/27, 139.219.17.0/24, 139.219.24.0/22, 139.219.145.0/27, 139.219.146.0/24, 139.219.156.0/22, 2406:e500:4420::/43, 2406:e500:4440::/43, 2406:e500:c020::/44, 2406:e500:c120::/44	TCP: 25, 443, 53, 80
12	Default Required	No	attachments.office365- net.cn	TCP: 443, 80

SharePoint Online and OneDrive for Business

ID	CATEGORY	ER	ADDRESSES	PORTS
4	Allow Required	No	*.partner.microsoftonl- *.sharepoint.cn 40.73.129.0/24, 40.73.161.0/24, 42.159.34.0/27, 42.159.38.0/23, 42.159.162.0/27, 42.159.166.0/23, 2406:e500:4000:2::/63, 2406:e500:4101:2::/64	TCP: 443, 80

Skype for Business Online and Microsoft Teams

ID	CATEGORY	ER	ADDRESSES	PORTS
3	Optimize Required	No	*.partner.lync.cn 42.159.34.32/27, 42.159.34.64/27, 42.159.34.96/28, 42.159.162.32/27, 42.159.162.64/27, 42.159.162.96/28	TCP: 443, 80

Microsoft 365 Common and Office Online

ID	CATEGORY	ER	ADDRESSES	PORTS
6	Allow Required	No	webshell.suite.partner.microsoftonline.cn 40.73.248.8/32, 40.73.252.10/32	TCP: 443, 80
7	Allow Required	No	*.azure-mobile.cn, *.chinacloudapp.cn, *.chinacloudapp.cn, *.chinacloud- mobile.cn, *.chinacloudsites.cn, *.partner.microsoftonline-m.cn, *.partner.microsoftonline-m.net.cn, *.partner.microsoftonline-m-i.cn, *.partner.microsoftonline-m-i.net.cn, *.partner.microsoftonline-p.net.cn, *.partner.microsoftonline-p-i.cn, *.partner.microsoftonline-p-i.net.cn, *.partner.officewebapps.cn, *.windowsazure.cn, partner.outlook.cn, portal.partner.microsoftonline.cdnsvc.com, r4.partner.outlook.cn 23.236.126.0/24, 42.159.224.122/32, 42.159.233.91/32, 42.159.237.146/32, 42.159.238.120/32, 58.68.168.0/24, 112.25.33.0/24, 123.150.49.0/24, 125.65.247.0/24, 139.217.17.219/32, 139.217.19.156/32, 139.217.21.3/32, 139.217.25.244/32, 171.107.84.0/24, 180.210.232.0/24, 180.210.234.0/24, 209.177.86.0/24, 209.177.90.0/24, 209.177.94.0/24, 222.161.226.0/24	TCP: 443, 80
8	Allow Required	No	*.onmschina.cn, *.partner.microsoftonline.net.cn, *.partner.microsoftonline-i.cn, *.partner.microsoftonline- i.net.cn, *.partner.office365.cn 101.28.252.0/24, 115.231.150.0/24, 123.235.32.0/24, 171.111.154.0/24, 175.6.10.0/24, 180.210.229.0/24, 211.90.28.0/24	TCP: 443, 80
9	Allow Required	No	*.partner.microsoftonline-p.cn 42.159.4.68/32, 42.159.4.200/32, 42.159.7.156/32, 42.159.132.138/32, 42.159.133.17/32, 42.159.135.78/32, 182.50.87.0/24	TCP: 443, 80
10	Allow Required	No	*.partner.microsoftonline-p.cn 42.159.4.68/32, 42.159.4.200/32, 42.159.7.156/32, 42.159.132.138/32, 42.159.133.17/32, 42.159.135.78/32, 103.9.8.0/22	TCP: 443, 80

ID	CATEGORY	ER	ADDRESSES	PORTS
11	Allow Required	No	activation.sls.microsoft.com, bjb-odcsm.officeapps.partner.office365.cn, bjb-ols.officeapps.partner.office365.cn, bjb-roaming.officeapps.partner.office365.cn, crl.microsoft.com, odc.officeapps.live.com, office15client.microsoft.com, officecdn.microsoft.com, ols.officeapps.partner.office365.cn, osi-prod-bjb01-odcsm.chinacloudapp.cn, osiprod-scus01-odcsm.cloudapp.net, osi-prod-sha01-odcsm.chinacloudapp.cn, roaming.officeapps.partner.office365.cn, sha-odcsm.officeapps.partner.office365.cn, sha-ols.officeapps.partner.office365.cn, sha-roaming.officeapps.partner.office365.cn 40.73.248.0/21, 42.159.4.45/32, 42.159.4.50/32, 42.159.4.225/32, 42.159.7.13/32, 42.159.132.73/32, 42.159.132.74/32, 42.159.132.75/32, 65.52.98.231/32, 65.55.69.140/32, 65.55.227.140/32, 70.37.81.47/32, 168.63.252.62/32	TCP: 443, 80
13	Default Required	No	*.msauth.cn, *.msauthimages.cn, *.msftauth.cn, *.msftauthimages.cn	TCP: 443, 80
15	Default Required	No	loki.office365.cn	TCP: 443
16	Default Required	No	*.cdn.office.net, shellprod.msocdn.com	TCP: 443
17	Allow Required	No	*.auth.microsoft.cn, login.partner.microsoftonline.cn, microsoftgraph.chinacloudapi.cn 40.72.70.0/23, 42.159.87.106/32, 42.159.92.96/32, 52.130.2.32/27, 52.130.3.64/27, 52.130.17.192/27, 52.130.18.32/27, 139.217.115.121/32, 139.217.118.25/32, 139.217.118.46/32, 139.217.118.54/32, 139.217.228.95/32, 139.217.231.198/32, 139.217.231.208/32, 139.217.231.219/32, 139.219.132.56/32, 139.219.133.182/32, 2406:e500:5500::/48	TCP: 443, 80
18	Default Required	No	*.aadrm.cn, *.protection.partner.outlook.cn	

Content Delivery Networks (CDNs)

10/28/2022 • 12 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

CDNs help keep Office 365 fast and reliable for end users. Cloud services like Office 365 use CDNs to cache static assets closer to the browsers requesting them to speed up downloads and reduce perceived end user latency. The information in this topic will help you learn about Content Delivery Networks (CDNs) and how they're used by Office 365.

What exactly is a CDN?

A CDN is a geographically distributed network consisting of proxy and file servers in datacenters connected by high-speed backbone networks. CDNs are used to reduce latency and load times for a specified set of files and objects in a web site or service. A CDN may have many thousands of endpoints for optimal servicing of incoming requests from any location.

CDNs are commonly used to provide faster downloads of generic content for a web site or service such as Javascript files, icons and images, and can also provide private access to user content such as files in SharePoint Online document libraries, streaming media files, and custom code.

CDNs are used by most enterprise cloud services. Cloud services like Office 365 have millions of customers downloading a mix of proprietary content (such as emails) and generic content (such as icons) at one time. It's more efficient to put images everyone uses, like icons, as close to the user's computer as possible. It isn't practical for every cloud service to build CDN datacenters that store this generic content in every metropolitan area, or even in every major Internet hub around the world, so some of these CDNs are shared.

How do CDNs make services work faster?

Downloading common objects like site images and icons over and over again can take up network bandwidth that can be better used for downloading important personal content, like email or documents. Because Office 365 uses an architecture that includes CDNs, the icons, scripts, and other generic content can be downloaded from servers closer to client computers, making the downloads faster. This means faster access to your personal content, which is securely stored in Office 365 datacenters.

CDNs help to improve cloud service performance in several ways:

- CDNs shift part of the network and file download burden away from the cloud service, freeing up cloud service resources for serving user content and other services by reducing the need to serve requests for static assets.
- CDNs are purpose built to provide low-latency file access by implementing high performance networks and file servers, and by leveraging updated network protocols such as [HTTP/2](#) with highly efficient compression and request multiplexing.
- CDN networks use many globally distributed endpoints to make content available as close as possible to users.

The Office 365 CDN

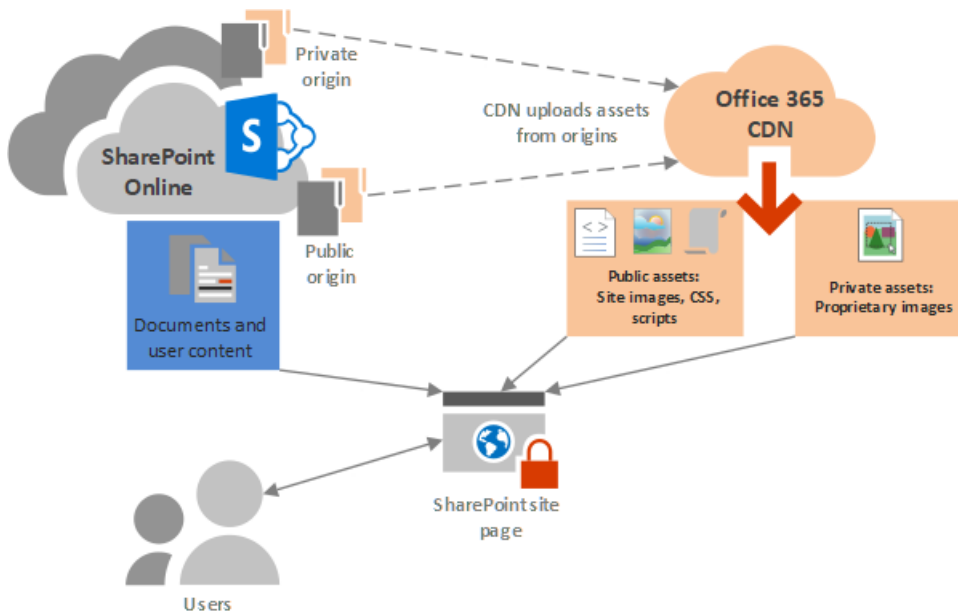
The built-in Office 365 Content Delivery Network (CDN) allows Office 365 administrators to provide better performance for their organization's SharePoint Online pages by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. The Office 365 CDN uses the [HTTP/2](#)

[protocol](#) for improved compression and download speeds.

NOTE

The Office 365 CDN is only available to tenants in the **Production** (worldwide) cloud. Tenants in the US Government, China and Germany clouds do not currently support the Office 365 CDN.

The Office 365 CDN is composed of multiple CDNs that allow you to host static assets in multiple locations, or *origins*, and serve them from global high-speed networks. Depending on the kind of content you want to host in the Office 365 CDN, you can add **public** origins, **private** origins or both.



Content in **public** origins within the Office 365 CDN is accessible anonymously, and can be accessed by anyone who has URLs to hosted assets. Because access to content in public origins is anonymous, you should only use them to cache non-sensitive generic content such as Javascript files, scripts, icons and images. The Office 365 CDN is used by default for downloading generic resource assets like the Office 365 client applications from a public origin.

Private origins within the Office 365 CDN provide private access to user content such as SharePoint Online document libraries, sites and proprietary images. Access to content in private origins is secured with dynamically generated tokens so it can only be accessed by users with permissions to the original document library or storage location. Private origins in the Office 365 CDN can only be used for SharePoint Online content, and you can only access assets through redirection from your SharePoint Online tenant.

The Office 365 CDN service is included as part of your SharePoint Online subscription.

For more information about how to use the Office 365 CDN, see [Use the Office 365 content delivery network with SharePoint Online](#).

To watch a series of short videos that provide conceptual and HOWTO information about using the Office 365 CDN, visit the [SharePoint Developer Patterns and Practices YouTube channel](#).

Other Microsoft CDNs

Although not a part of the Office 365 CDN, you can use these CDNs in your Office 365 tenant for access to SharePoint development libraries, custom code and other purposes that fall outside the scope of the Office 365 CDN.

Azure CDN

NOTE

Beginning in Q3 2020, SharePoint Online will begin caching videos on the Azure CDN to support improved video playback and reliability. Popular videos will be streamed from the CDN endpoint closest to the user. This data will remain within the Microsoft Purview boundary. This is a free service for all tenants and it does not require any customer action to configure.

You can use the **Azure CDN** to deploy your own CDN instance for hosting custom web parts, libraries and other resource assets, which allows you to apply access keys to your CDN storage and exert greater control over your CDN configuration. Use of the Azure CDN isn't free, and requires an Azure subscription.

For more information on how to configure an Azure CDN instance, see [Quickstart: Integrate an Azure storage account with Azure CDN](#).

For an example of how the Azure CDN can be used to host SharePoint web parts, see [Deploy your SharePoint client-side web part to Azure CDN](#).

For information about the Azure CDN PowerShell module, see [Manage Azure CDN with PowerShell](#).

Microsoft Ajax CDN

Microsoft's **Ajax CDN** is a read-only CDN that offers many popular development libraries including jQuery (and all of its other libraries), ASP.NET Ajax, Bootstrap, Knockout.js, and others.

To include these scripts in your project, simply replace any references to these publicly available libraries with references to the CDN address instead of including it in your project itself. For example, use the following code to link to jQuery:

```
<script src=https://ajax.aspnetcdn.com/ajax/jquery-2.1.1.js> </script>
```

For more information about how to use the Microsoft Ajax CDN, see [Microsoft Ajax CDN](#).

How does Office 365 use content from a CDN?

Regardless of what CDN you configure for your Office 365 tenant, the basic data retrieval process is the same.

1. Your client (a browser or Office client application) requests data from Office 365.
2. Office 365 either returns the data directly to your client or, if the data is part of a set of content hosted by the CDN, redirects your client to the CDN URL.
 - a. If the data is already cached in a *public* origin, your client downloads the data directly from the nearest CDN location to your client.
 - b. If the data is already cached in a *private* origin, the CDN service checks your Office 365 user account's permissions on the origin. If you have permissions, SharePoint Online dynamically generates a custom URL composed of the path to the asset in the CDN and two access tokens, and returns the custom URL to your client. Your client then downloads the data directly from the nearest CDN location to your client using the custom URL.
3. If the data isn't cached at the CDN, the CDN node requests the data from Office 365 and then caches the data for time after your client downloads the data.

The CDN figures out the closest datacenter to the user's browser and, using redirection, downloads the requested data from there. CDN redirection is quick, and can save users a lot of download time.

How should I set up my network so that CDNs work best with Office 365?

Minimizing latency between clients on your network and CDN endpoints is the key consideration for ensuring optimal performance. You can use the best practices outlined in [Managing Office 365 endpoints](#) to ensure that your network configuration permits client browsers to access the CDN directly rather than routing CDN traffic through central proxies to avoid introducing unnecessary latency.

You can also read [Office 365 Network Connectivity Principles](#) to understand the concepts behind optimizing Office 365 network performance.

Is there a list of all the CDNs that Office 365 uses?

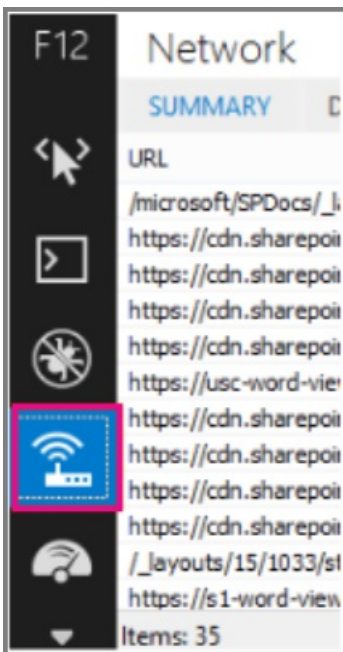
The CDNs in use by Office 365 are always subject to change and in many cases there are multiple CDN partners configured in the event one is unavailable. The primary CDNs used by Office 365 are:

CDN	COMPANY	USAGE	LINK
Office 365 CDN	Microsoft Azure	Generic assets in public origins, SharePoint user content in private origins	Microsoft Azure CDN
Azure CDN	Microsoft	Custom code, SharePoint Framework solutions	Microsoft Azure CDN
Microsoft Ajax CDN (read only)	Microsoft	Common libraries for Ajax, jQuery, ASP.NET, Bootstrap, Knockout.js etc.	Microsoft Ajax CDN

What performance gains does a CDN provide?

There are many factors involved in measuring specific differences in performance between data downloaded directly from Office 365 and data downloaded from a specific CDN, such as your location relative to your tenant and to the nearest CDN endpoint, the number of assets on a page that are served by the CDN, and transient changes in network latency and bandwidth. However, a simple A/B test can help to show the difference in download time for a specific file.

The following screenshots illustrate the difference in download speed between the native file location in Office 365 and the same file hosted on the [Microsoft Ajax Content Delivery Network](#). These screenshots are from the **Network** tab in the Internet Explorer 11 developer tools. These screenshots show the latency on the popular library jQuery. To bring up this screen, in Internet Explorer, press F12 and select the **Network** tab, which is symbolized with a Wi-Fi icon.



This screenshot shows the library uploaded to the master page gallery on the SharePoint Online site itself. The time it took to upload the library is 1.51 seconds.

URL	Received	Taken	Initiator
/_catalogs/masterpage/javascript/jquery-2.1.1.min.js	82.98 KB	1.51 s	<script>
https://cdn.sharepointonline.com/12413/_layouts/15/16	18.98 KB	156 ms	<script>
/ScriptResource.axd?d=M1vNi_a6A2vtkOenP45i9-peGfx	100.80 KB	2.04 s	<script>

The second screenshot shows the same file delivered by Microsoft's CDN. This time the latency is around 496 milliseconds. This is a large improvement and shows that a whole second is shaved off the total time to download the object.

URL	Received	Taken
https://ajax.aspnetcdn.com/ajax/jquery/jquery-2.1.1.min.js	82.74 KB	469 ms
/WebResource.axd?d=nMv/y4UjLBwmUSt-GLxLgIVJy4RM4FI/qCK2olh3D5kBMxz5dwm5KllpDx9vM8MKztZon...	22.33 KB	0.84 s
/_layouts/15/images/spcommon.png?rev=38	20.56 KB	1.15 s

Is my data safe?

We take great care to protect the data that runs your business. Data stored in the Office 365 CDN is encrypted both in transit and at rest, and access to data in the Office 365 SharePoint CDN is secured by Office 365 user permissions and token authorization. Requests for data in the Office 365 SharePoint CDN must be referred (redirected) from your Office 365 tenant or an authorization token won't be generated.

To ensure that your data remains secure, we recommend that you never store user content or other sensitive data in a public CDN. Because access to data in a public CDN is anonymous, public CDNs should only be used to host generic content such as web script files, icons, images and other non-sensitive assets.

NOTE

3rd party CDN providers may have privacy and compliance standards that differ from the commitments outlined by the Office 365 Trust Center. Data cached through the CDN service may not conform to the Microsoft Data Processing Terms (DPT), and may be outside of the Office 365 Trust Center compliance boundaries.

For in-depth information about privacy and data protection for Office 365 CDN providers, visit the following:

- Learn more about Office 365 privacy and data protection at the [Microsoft Trust Center](#)

- Learn more about Akamai's privacy and data protection at the [Akamai Privacy Trust Center](#)
- Learn more about Azure privacy and data protection at the [Azure Trust Center](#)

How can I secure my network with all these 3rd party services?

Using an extensive set of partner services allows Office 365 to scale and meet availability requirements and enhance the user experience when using Office 365. The 3rd party services Office 365 leverages include both certificate revocation lists; such as [crl.microsoft.com](#) or [sa.symcb.com](#), and CDNs; such as [r3.res.outlook.com](#). Every CDN FQDN generated by Office 365 is a custom FQDN for Office 365. If you're sent to a FQDN at the request of Office 365, you can be assured that the CDN provider controls the FQDN and the underlying content at that location.

For customers that want to segregate requests destined for a Microsoft or Office 365 datacenter from requests that are destined for a 3rd party, we've written up guidance on [Managing Office 365 endpoints](#).

Is there a list of all the FQDNs that leverage CDNs?

The list of FQDNs and how they leverage CDNs change over time. Refer to our published [Office 365 URLs and IP address ranges](#) page to get up to date on the latest FQDNs that leverage CDNs.

You can also use the [Office 365 IP Address and URL Web service](#) to request the current Office 365 URLs and IP address ranges formatted as CSV or JSON.

Can I use my own CDN and cache content on my local network?

We're continually looking for new ways to support our customers' needs and are currently exploring the use of caching proxy solutions and other on-premises CDN solutions.

Although it isn't a part of the Office 365 CDN, you can also use the **Azure CDN** for hosting custom web parts, libraries and other resource assets, which allows you to apply access keys to your CDN storage and exert greater control over your CDN configuration. Use of the Azure CDN isn't free, and requires an Azure subscription. For more information on how to configure an Azure CDN instance, see [Quickstart: Integrate an Azure storage account with Azure CDN](#).

I'm using Azure ExpressRoute for Office 365, does that change things?

[Azure ExpressRoute for Office 365](#) provides a dedicated connection to Office 365 infrastructure that is segregated from the public internet. This means that clients will still need to connect over non-ExpressRoute connections to connect to CDNs and other Microsoft infrastructure that isn't explicitly included in the list of services supported by ExpressRoute. For more information about how to route specific traffic such as requests destined for CDNs, see [Office 365 network traffic management](#).

Can I use CDNs with SharePoint Server on-premises?

Using CDNs only makes sense in a SharePoint Online context and should be avoided with SharePoint Server. This is because all of the advantages around geographic location don't hold true if the server is located on-premises or geographically close anyway. Additionally, if there's a network connection to the servers where it's hosted, then the site may be used without an Internet connection and therefore can't retrieve the CDN files. Otherwise, you should use a CDN if there's one available and stable for the library and files you need for your site.

Here's a short link you can use to come back: <https://aka.ms/o365cdns>

See also

[Office 365 Network Connectivity Principles](#)

[Assessing Office 365 network connectivity](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Use the Office 365 content delivery network with SharePoint Online](#)

[Microsoft Trust Center](#)

[Tune Office 365 performance](#)

IPv6 support in Microsoft 365 services

10/28/2022 • 2 minutes to read • [Edit Online](#)

With the growing adoption and support of IPv6 across enterprise networks, service providers, and devices, many customers are wondering if their users can continue to access Microsoft 365 services from IPv6 clients and IPv6 networks. Microsoft 365 services can be successfully used from both IPv6 dual stack and IPv6-only devices (IPv6-only devices require translation technologies such as DNS64 or NAT64). In fact, we have an increasing number of customers, from consumers to large enterprises, who are moving towards greater adoption of IPv6. For most customers, IPv4 won't completely disappear from their digital landscape, so we aren't planning to require IPv6 or to de-prioritize IPv4 in any Microsoft 365 features or services.

One of our key priorities with Microsoft 365 is to ensure seamless customer and user experiences over the Internet from any location, from any device. This includes access to Microsoft 365 from customer devices that are using IPv6 in the dual stack configuration as well as transitioning to IPv6-only client deployments. In most cases, when you follow a standard Internet-based model of connecting to Microsoft 365 as described in [Microsoft 365 network connectivity principles](#), [Microsoft 365 URLs and IP address ranges](#), and [Microsoft 365 network planning best practices](#), IPv6 transitions won't be disruptive to your user experience.

Many Microsoft 365 services already provide native IPv6 support today and can be accessed directly from IPv6 dual stack and IPv6-only clients. Microsoft 365 also allows access through conventional IPv6 to IPv4 translation technologies (such as base 64 proxies or DNS64/NAT64) commonly used by customers and network solution providers to connect to IPv4 Internet resources.

As with any SaaS service and the Internet overall, the scope of natively IPv6 enabled Microsoft 365 interfaces, features and APIs expands continuously and without direct customer action or control. If you're running IPv6 or IPv6-only services on your networks that need access to Microsoft 365 and the Internet, it is recommended that you include dynamic IPv6/IPv4 transitional mechanisms such as DNS64/NAT64 to ensure end-to-end IPv6 connectivity to Microsoft 365 without any further network reconfigurations.

Most of Microsoft 365 services have been or will be enabled with IPv6 capabilities completely transparently for end users and IT admins. Some Microsoft 365 scenarios (such as anonymous inbound e-mail) do have special requirements and considerations for use in conjunction with IPv6. For more details about scenario specific IPv6 requirements and considerations, please contact your Microsoft account team or Microsoft support.

Here's a short link you can use to come back: <https://aka.ms/o365ip6>

See also

[Microsoft 365 Network Connectivity Overview](#)

[Managing Office 365 endpoints](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 IP Address and URL Web service](#)

[Assessing Microsoft 365 network connectivity](#)

[Network planning and performance tuning for Microsoft 365](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Content Delivery Networks](#)

[Microsoft 365 connectivity test](#)

[How Microsoft builds its fast and reliable global network](#)

[Office 365 Networking blog](#)

NAT support with Office 365

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Previously, guidance suggested that the maximum number of Exchange clients you should use per IP address to connect to Office 365 was about 2,000 clients per network port.

Why use NAT?

By using NAT, thousands of people on a corporate network can "share" a few publicly routable IP addresses.

Most corporate networks use private (RFC1918) IP address space. Private address space is allocated by the Internet Assigned Numbers Authority (IANA) and intended solely for networks that do not route directly to and from the global Internet.

To provide Internet access to devices on a private IP address space, organizations use gateway technologies like firewalls and proxies that provide network address translation (NAT) or port address translation (PAT) services. These gateways make traffic from internal devices to the Internet (including Office 365) appear to be coming from one or more publicly routable IP addresses. Each outbound connection from an internal device translates to a different source TCP port on the public IP address.

Why do you need to have so many connections open to Office 365 at the same time?

Outlook may open eight or more connections (in situations where there are add-ins, shared calendars, mailboxes, etc.). Because there are a maximum of 64,000 ports available on a Windows-based NAT device, there can be a maximum of 8,000 users behind an IP address before the ports are exhausted. Note that if customers are using non-Windows OS-based devices for NAT, the total available ports are dependent on what NAT device or software is being used. In this scenario, the maximum number of ports could be less than 64,000. Availability of ports is also affected by other factors such as Windows restricting 4,000 ports for its own use, which reduces the total number of available ports to 60,000. There may be other applications, such as Internet Explorer, that could connect at the same time, requiring additional ports.

Calculating maximum supported devices behind a single public IP address with Office 365

To determine the maximum number of devices behind a single public IP address, you should monitor network traffic to determine peak port consumption per client. Also, a peak factor should be used for the port usage (minimum 4).

Use the following formula to calculate the number of supported devices per IP address:

Maximum supported devices behind a single public IP address = $(64,000 - \text{restricted ports}) / (\text{Peak port consumption} + \text{peak factor})$

For example, if the following were true:

- **Restricted ports:** 4,000 for the operating system
- **Peak port consumption:** 6 per device

- **Peak factor:** 4

Then, the maximum supported devices behind a single public IP address = $(64,000 - 4,000)/(6 + 4) = 6,000$

With the release of Office 365 hosting pack, included in the updates from September 2011 for Microsoft Office Outlook 2007, or November 2011 for Microsoft Outlook 2010, or a later update, the number of connections from Outlook (both Office Outlook 2007 with Service Pack 2 and Outlook 2010) to Exchange can be as few as 2. You'll need to factor in the different operating systems, user behaviors, and so on to determine the minimum and maximum number of ports that your network will require at peak.

If you want to support more devices behind a single public IP address, follow the steps outlined to assess the maximum number of devices that can be supported:

Monitor network traffic to determine peak port consumption per client. You should collect this data:

- From multiple locations
- From multiple devices
- At multiple times

Use the preceding formula to calculate the maximum users per IP address that can be supported in their environment.

There are various methods for distributing client load across additional public IP addresses. Strategies available depend on the capabilities of the corporate gateway solution. The simplest solution is to segment your user address space and statically "assign" a number of IP addresses to each gateway. Another alternative that many gateway devices offer is the ability to use a pool of IP addresses. The benefit of the address pool is that it is much more dynamic and less likely to require adjustment as your user base grows.

See also

[Managing Office 365 endpoints](#)

[Office 365 endpoints FAQ](#)

Network requests in Office for Mac

10/28/2022 • 10 minutes to read • [Edit Online](#)

Office for Mac applications provide a native app experience on the macOS platform. Each app is designed to work in a variety of scenarios, including states when no network access is available. When a machine is connected to a network, the applications automatically connect to a series of web-based services to provide enhanced functionality. The following information describes which endpoints and URLs the applications try to reach, and the services provided. This information is useful when troubleshooting network configuration issues and setting policies for network proxy servers. The details in this article are intended to complement the [Office 365 URL and address ranges article](#), which includes endpoints for computers running Microsoft Windows. Unless noted, the information in this article also applies to Office 2019 for Mac and Office 2016 for Mac, which are available as a one-time purchase from a retail store or through a volume licensing agreement.

Most of this article is tables detailing network URLs, type, and description of service or feature provided by that endpoint. Each of the Office apps may differ in its service and endpoint usage. The following apps are defined in the tables below:

- W: Word
- P: PowerPoint
- X: Excel
- O: Outlook
- N: OneNote

The URL type is defined as follows:

- ST: Static - The URL is hard-coded into the client application.
- SS: Semi-Static - The URL is encoded as part of a web page or redirector.
- CS: Config Service - The URL is returned as part of the Office Configuration Service.

Office for Mac default configuration

Installation and updates

The following network endpoints are used to download the Office for Mac installation program from the Microsoft Content Delivery Network (CDN).

URL	TYPE	DESCRIPTION
<code>https://go.microsoft.com/fwlink/</code>	ST	Microsoft 365 Installation Portal forward link service to latest installation packages.
<code>https://officecdn-microsoft-com.akamaized.net/</code>	SS	Location of installation packages on the Content Delivery Network.
<code>https://officecdn.microsoft.com/</code>	SS	Location of installation packages on the Content Delivery Network.
<code>https://officeci-mauservice.azurewebsites.net/</code>	ST	Management Control endpoint for Microsoft AutoUpdate

First app launch

The following network endpoints are contacted on first launch of an Office app. These endpoints provide enhanced Office functionality for users, and the URLs are contacted regardless of license type (including Volume License installations).

URL	APPS	TYPE	DESCRIPTION
https://config.edge.skype.com/	WXPON	ST	'Flighting' Configuration - allows for feature light-up and experimentation.
https://ocos-office365-s2s.msedge.net/	WXPON	ST	'Flighting' Network Configuration Test
https://client-office365-tas.msedge.net/	WXPON	ST	'Flighting' Network Configuration Test
https://officeclient.microsoft.com/	WXPON	ST	Office Configuration Service - Master list of service endpoints.
https://nexusrules.officeapps.live.com/	WXPON	ST	Office Rules Telemetry download - Informs the client about what data and events to upload to the telemetry service.
https://mobile.pipe.aria.microsoft.com/	None	CS	OneNote Telemetry Service
https://nexus.officeapps.live.com/	WXPON	ST	Office Telemetry Upload Reporting - "Heartbeat" and error events that occur on the client are uploaded to the telemetry service.
https://templateservice.officeapps.live.com/	WXP	CS	Office Template Service - Provides users with online document templates.
https://omextemplates.content.office.net/	WXP	CS	Office Templates Downloads - Storage of PNG template images.
https://store.office.com/	WXP	CS	Store configuration for Office apps.
https://odc.officeapps.live.com/	WXPON	CS	Office Document Integration Services Catalog (list of services and endpoints) and Home Realm Discovery.
https://cdn.odc.officeapps.live.com/	WXPON	CS	Resources for Home Realm Discovery v2 (15.40 and later)

URL	APPS	TYPE	DESCRIPTION
https://officecdn.microsoft.com/	WXPO	ST	Microsoft AutoUpdate Manifests - checks to see if there are updates available
https://ajax.aspnetcdn.com/	WXPO	SS	Microsoft Ajax JavaScript Library
https://wikipedia.firstpartyapps.oaspapps.com/	WXPO	SS	Wikipedia app for Office configuration and resources.
https://excelbingmap.firstpartyapps.oaspapps.com/	WXPO	SS	Bing Map app for Office configuration and resources.
https://peoplegraph.firstpartyapps.oaspapps.com/	WXPO	SS	People Graph app for Office configuration and resources.
https://www.onenote.com/	N	ST	What's New content for OneNote.
https://site-cdn.onenote.net/	N	ST	New content for OneNote.
https://site-cdn.onenote.net/	N	SS	What's New images for OneNote.
https://acompli.helpshift.com/	O	ST	In-app Support Service.
https://prod-global-autodetect.acompli.net/	O	ST	Email Account Detection Service.
https://autodiscover-s.outlook.com/	WXPO	ST	Outlook AutoDiscovery
https://outlook.office365.com/	WXPO	ST	Outlook endpoint for Microsoft 365 service.
https://r1.res.office365.com/	WXPO	ST	Icons for Outlook add-ins.

NOTE

The Office Configuration Service acts as an auto-discovery service for all Microsoft Office clients, not just for Mac. The endpoints returned in the response are semi-static in that change is very infrequent, but still possible.

Sign-in

The following network endpoints are contacted when signing in to cloud-based storage. Depending on your account type, different services may be contacted. For example:

- **MSA: Microsoft Account** - typically used for consumer and retail scenarios
- **OrgID: Organization Account** - typically used for commercial scenarios

URL	APPS	TYPE	DESCRIPTION
<code>https://login.windows.net/</code>	WXPON	ST	Windows Authorization Service
<code>https://login.microsoftonline.com/</code>	WXPON	ST	Microsoft 365 Login Service (OrgID)
<code>https://login.live.com/</code>	WXPON	ST	Microsoft Account Login Service (MSA)
<code>https://auth.gfx.ms/</code>	WXPON	CS	Microsoft Account Login Service Helper (MSA)
<code>https://secure.aadcdn.microsoftonline-p.com/</code>	WXPON	SS	Microsoft 365 Login Branding (OrgID)
<code>https://ocws.officeapps.live.com/</code>	WXPON	CS	Document and Places Storage Locator
<code>https://roaming.officeapps.live.com/</code>	WXPON	CS	Most Recently Used (MRU) document service

NOTE

For subscription-based and retail licenses, signing in both activates the product, and enables access to cloud resources such as OneDrive. For Volume License installations, users are still prompted to sign-in (by default), but that is only required for access to cloud resources, as the product is already activated.

Product activation

The following network endpoints apply to Microsoft 365 Subscription and Retail License activations. Specifically, this does NOT apply to Volume License installations.

URL	APPS	TYPE	DESCRIPTION
<code>https://ols.officeapps.live.com/</code>	WXPON	CS	Office Licensing Service

What's New content

The following network endpoints apply to Microsoft 365 Subscription only.

URL	APPS	TYPE	DESCRIPTION
<code>https://contentstorage.osi.office.net/</code>	WXPON	SS	What's New JSON page content.

Researcher

The following network endpoints apply to Microsoft 365 Subscription only.

URL	APPS	TYPE	DESCRIPTION
<code>https://entity.osi.office.net/</code>	WXPON	CS	Researcher Web Service

URL	APPS	TYPE	DESCRIPTION
https://cdn.entity.osi.office.net/	W	CS	Researcher Static Content
https://www.bing.com/	W	CS	Researcher Content Provider

Smart Lookup

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

URL	APPS	TYPE	DESCRIPTION
https://uci.officeapps.live.com/	WXP	CS	Insights Web Service
https://ajax.googleapis.com/	WXP	CS	JQuery Library
https://cdnjs.cloudflare.com/	WXP	CS	Supporting JavaScript Library
https://www.bing.com/	WXP	CS	Insights Content Provider
https://tse1.mm.bing.net/	WXP	CS	Insights Content Provider

PowerPoint Designer

The following network endpoints apply to Microsoft 365 Subscription only.

URL	APPS	TYPE	DESCRIPTION
https://pptsgs.officeapps.live.com/	P	CS	PowerPoint Designer web service

PowerPoint QuickStarter

The following network endpoints apply to Microsoft 365 Subscription only.

URL	APPS	TYPE	DESCRIPTION
https://pptcts.officeapps.live.com/	P	CS	PowerPoint QuickStarter web service

Send a Smile/Frown

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

URL	APPS	TYPE	DESCRIPTION
https://sas.office.microsoft.com/	WXP	CS	Send a Smile Service

Contact Support

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License

activations.

URL	APPS	TYPE	DESCRIPTION
https://powerlift-frontdesk.acompli.net/	O	CS	Contact Support Service
https://acompli.helpshift.com/	O	CS	In-app Support Service

Save As PDF

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations.

URL	APPS	TYPE	DESCRIPTION
https://wordcs.officeapps.live.com/	W	CS	Word document conversion service (PDF)

Office Apps (aka add-ins)

The following network endpoints apply to both Microsoft 365 Subscription and Retail/Volume License activations when Office App add-ins are trusted.

URL	APPS	TYPE	DESCRIPTION
https://store.office.com/	WXPO	CS	Office app store configuration
https://wikipedia.firstpartyapps.oaspapps.com/	W	SS	Wikipedia app resources
https://excelbingmap.firstpartyapps.oaspapps.com/	X	SS	Bing Map app resources
https://peoplegraph.firstpartyapps.oaspapps.com/	X	SS	People Graph app resources
https://o15.officeredir.microsoft.com/	WPX	SS	Office Redirection Service
https://appsforoffice.microsoft.com/	WPX	SS	Office JavaScript Libraries
https://telemetry.firstpartyapps.oaspapps.com/	W	SS	Telemetry and Reporting Service for Office apps
https://ajax.microsoft.com/	W	SS	Microsoft Ajax JavaScript Library
https://ajax.aspnetcdn.com/	X	SS	Microsoft Ajax JavaScript Library
https://c.microsoft.com/	WPXO	SS	Office JavaScript Libraries
https://c1.microsoft.com/	WPXO	SS	Support resources
https://cs.microsoft.com/	WPXO	SS	Support resources

URL	APPS	TYPE	DESCRIPTION
https://c.bing.com/	WPXO	SS	Support resources
https://*.cdn.optimizely.com/	WPXO	SS	JavaScript library
https://errors.client.optimizely.com/	WPXO	SS	Error reporting
https://*-contentstorage.osi.office.net/	WPXO	SS	Font resources
https://nexus.ensighten.com/	WPXO	SS	Telemetry Service
https://browser.pipe.aria.microsoft.com/	WPXO	SS	Telemetry Reporting
https://*.vo.msecnd.net/	WPXO	SS	Microsoft Store Asset Library
https://*.wikipedia.org/	W	SS	Wikipedia page resources
https://upload.wikimedia.org/	W	SS	Wikipedia media resources
https://wikipedia.firstpartyapps.sandbox.oappsplatform.com/	W	SS	Wikipedia sandbox frame
https://*.virtualearth.net/	X	SS	Map templates

Safe Links

The following network endpoint applies to all Office applications for Microsoft 365 Subscription only.

URL	TYPE	DESCRIPTION
https://*.oscs.protection.outlook.com/	CS	Microsoft Safe Link Service

Crash reporting

The following network endpoint applies to all Office applications for both Microsoft 365 Subscription and Retail/Volume License activations. When a process unexpectedly crashes, a report is generated and sent to the Watson service.

URL	TYPE	DESCRIPTION
https://watson.microsoft.com/	ST	Microsoft Error Reporting Service
https://officeci.azurewebsites.net/	ST	Office Collaborative Insights Service

Options for reducing network requests and traffic

The default configuration of Office for Mac provides the best user experience, both in terms of functionality and keeping the machine up to date. In some scenarios, you may wish to prevent applications from contacting network endpoints. This section discusses options for doing so.

Disabling Cloud Sign-In and Office Add-Ins

Volume License customers may have strict policies about saving documents to cloud-based storage. The following per-application preference can be set to disable MSA/OrgID Sign in, and access to Office Add-ins.

- `defaults write com.microsoft.Word UseOnlineContent -integer 0`
- `defaults write com.microsoft.Excel UseOnlineContent -integer 0`
- `defaults write com.microsoft.Powerpoint UseOnlineContent -integer 0`

If users try to access the Sign-In function, they will see an error that a network connection is not present. Because this preference also blocks online product activation, it should only be used for Volume License installations. Specifically, using this preference will prevent Office applications from accessing the following endpoints:

- `https://odc.officeapps.live.com`
- `https://*.firstpartyapps.oaspapps.com`
- All endpoints listed in the 'Sign In' section above.
- All endpoints listed in the 'Smart Lookup' section above.
- All endpoints listed in the 'Product Activation' section above.
- All endpoints listed in the 'Office Apps (aka add-ins)' section above.

To re-establish full functionality for the user, either set the preference to '2' or remove it.

NOTE

This preference requires Office for Mac build 15.25 [160726] or later.

Telemetry

Office for Mac sends telemetry information back to Microsoft at regular intervals. Data is uploaded to the 'Nexus' endpoint. The telemetry data helps the engineering team assess the health and any unexpected behaviors of each Office app. There are two categories of telemetry:

- **Heartbeat** contains version and license information. This data is sent immediately upon app launch.
- **Usage** contains information about how apps are being used and non-fatal errors. This data is sent every 60 minutes.

Microsoft takes your privacy very seriously. You can read about Microsoft's data collection policy at <https://privacy.microsoft.com>. To prevent applications from sending 'Usage' telemetry, the **SendAllTelemetryEnabled** preference can be adjusted. The preference is per-application, and can be set via macOS Configuration Profiles, or manually from Terminal:

```
defaults write com.microsoft.Word SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Excel SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Powerpoint SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Outlook SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.onenote.mac SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.autoupdate2 SendAllTelemetryEnabled -bool FALSE
```

```
defaults write com.microsoft.Office365ServiceV2 SendAllTelemetryEnabled -bool FALSE
```

Heartbeat telemetry is always sent and cannot be disabled.

Crash reporting

When a fatal application error occurs, the application will unexpectedly terminate and upload a crash report to the 'Watson' service. The crash report consists of a call-stack, which is the list of steps the application was processing leading up to the crash. These steps help the engineering team identify the exact function that failed and why.

In some cases, the contents of a document will cause the application to crash. If the app identifies the document as the cause, it will ask the user if it's okay to also send the document along with the call-stack. Users can make an informed choice to this question. IT administrators may have strict requirements about the transmission of documents and make the decision on behalf of the user to never send documents. The following preference can be set to prevent documents from being sent, and to suppress the prompt to the user:

```
defaults write com.microsoft.errorreporting IsAttachFilesEnabled -bool FALSE
```

NOTE

If **SendAllTelemetryEnabled** is set to **FALSE**, all crash reporting for that process is disabled. To enable crash reporting without sending usage telemetry, the following preference can be set:

```
defaults write com.microsoft.errorreporting IsMerpEnabled -bool TRUE
```

Updates

Microsoft releases Office for Mac updates at regular intervals (typically once a month). We strongly encourage users and IT administrators to keep machines up to date to ensure the latest security fixes are installed. In cases where IT administrators want to closely control and manage machine updates, the following preference can be set to prevent the AutoUpdate process from automatically detecting and offering product updates:

```
defaults write com.microsoft.autoupdate2 HowToCheck -string 'Manual'
```

Blocking Requests with a Firewall/Proxy

If your organization blocks requests to URLs via a firewall or proxy server be sure to configure the URLs listed in this document as either allowed, or block listed with a 40X response (e.g. 403 or 404). A 40X response will allow the Office applications to gracefully accept the inability to access the resource, and will provide a faster user experience, than simply dropping the connection, which in turn will cause the client to retry.

If your proxy server requires authentication, a 407 response will be returned to the client. For the best experience, ensure that you're using Office for Mac builds 15.27 or later, as they include specific fixes for working with NTLM and Kerberos servers.

See also

[Office 365 URLs and IP address ranges](#)

Network planning and performance tuning for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

Before you deploy for the first time or migrate to Microsoft 365, you can use the information in these topics to estimate the bandwidth you need and then to test and verify that you have enough bandwidth to deploy or migrate to Microsoft 365. For an overview, see: [Network and migration planning for Microsoft 365](#).

CATEGORY	DESCRIPTION	CATEGORY	DESCRIPTION
Network planning 	Want fast connections and pages that load quickly? Read Getting the best connectivity and performance in Microsoft 365 . Read Microsoft 365 Network Connectivity Overview to understand concepts.	Measuring your network 	Read Microsoft 365 performance tuning using baselines and performance history and Performance troubleshooting plan for Microsoft 365 . Use these tools to evaluate your existing network .
Best practices 	Best practices for network planning and improving migration performance for Microsoft 365 . Want to get started helping your users right away? See Best practices for using Office 365 on a slow network . Microsoft 365 Network Connectivity Principles will help you understand the most recent guidance for securely optimizing Microsoft 365 network connectivity.	Reference 	Want the details, like a list of IP addresses and ports? See the Network planning reference for Microsoft 365 .
	For the steps to optimize your network for Microsoft 365 and other Microsoft cloud platforms and services, see the Microsoft Cloud Networking for Enterprise Architects poster.		

Performance tuning and troubleshooting resources for Microsoft 365

Once you have Microsoft 365 deployed, you can optimize your performance by using the topics in this section. If you experience performance degradation you can also use these topics to troubleshoot issues.

Tune Office 365 performance: For information about using network address translation with Office 365, see [NAT support with Office 365](#). Also, take a look at the [top 10 tips for optimizing and troubleshooting your Office 365 network connectivity](#).

Tune Exchange Online performance: Use these articles to fine tune Exchange Online performance.

Prepare your organization's network for Microsoft Teams: Use these articles to optimize your network for Teams.

Tune Skype for Business Online performance: Use these articles to fine tune Skype for Business Online performance.

Tune SharePoint Online performance: Use these articles to fine tune SharePoint Online performance.

Tune Project Online performance: Use this article to fine tune Project Online performance

Monitor Microsoft 365 connectivity

10/28/2022 • 2 minutes to read • [Edit Online](#)

Once you've deployed Microsoft 365, you can maintain Microsoft 365 connectivity using some of the tools and techniques below. You'll want to understand the official [Service Health and Continuity](#) guidelines as well as our [Best practices for using Microsoft 365 on a slow network](#). You'll also want to grab the [Microsoft 365 admin app](#) and bookmark our [Microsoft 365 for business - Admin Help](#).

Monitoring Microsoft 365 Connectivity

TYPE OF MONITORING	DESCRIPTION
Getting notified of new Microsoft 365 endpoints	If you're Managing Microsoft 365 endpoints , you'll want to receive notifications when we publish new endpoints, you can subscribe to our RSS feed using your favorite RSS reader. Here is how to subscribe via Outlook or you can have the RSS feed updates emailed to you .
Use System Center to Monitor Microsoft 365	If you're using Microsoft System Center, you can download the Microsoft System Center Operations Manager Management Pack for Microsoft 365 to begin monitoring Microsoft 365 today. For more detailed guidance, please see the management pack operations guide.
Monitoring the health of Azure ExpressRoute	If you are connecting to Microsoft 365 using Azure ExpressRoute for Microsoft 365, you'll want to ensure that you're using both the Microsoft 365 Service Health Dashboard as well as the Azure Reducing troubleshooting time with Azure Resource health
Using Azure AD Connect Health with AD FS	If you're using AD FS for Single Sign-On with Microsoft 365, you'll want to begin using Azure AD Connect Health to monitor your AD FS infrastructure .
Programmatically monitor Microsoft 365	Refer to our guidance on the Microsoft 365 Management API .

Here's a short link you can use to come back: <https://aka.ms/monitorconnectivity365>

Related topics

[Configure Microsoft 365 Enterprise services and applications](#)

[Get your organization ready for Microsoft 365 Enterprise](#)

[Network planning and performance tuning for Microsoft 365](#)

[Microsoft 365 integration with on-premises environments](#)

[Managing Microsoft 365 endpoints](#)

Managing ExpressRoute for Office 365 connectivity

10/28/2022 • 5 minutes to read • [Edit Online](#)

ExpressRoute for Office 365 offers an alternative routing path to reach many Office 365 services without needing all traffic to egress to the internet. Although the internet connection to Office 365 is still needed, the specific routes that Microsoft advertises through BGP to your network make the direct ExpressRoute circuit preferred unless there are other configurations in your network. The three common areas you may want to configure to manage this routing include prefix filtering, security, and compliance.

NOTE

Microsoft changed how the Microsoft Peering routing domain is reviewed for Azure ExpressRoute. Starting July 31st, 2017, all Azure ExpressRoute customers can enable Microsoft Peering directly from the Azure Administrative console or via PowerShell. After enabling Microsoft Peering, any customer can create route filters to receive BGP route advertisements for Dynamics 365 Customer Engagement applications (Formerly known as CRM Online). Customers needing Azure ExpressRoute for Office 365 must obtain review from Microsoft before they can create route filters for Office 365. Please contact your Microsoft Account team to learn about how to request a review for enabling Office 365 ExpressRoute. Unauthorized subscriptions trying to create route filters for Office 365 will receive an [error message](#)

Prefix filtering

Microsoft recommends that customers accept all BGP routes as advertised from Microsoft, the routes provided undergo a rigorous review and validation process removing any benefits to added scrutiny. ExpressRoute natively offers the recommended controls such as IP prefix ownership, integrity, and scale - with no inbound route filtering on the customer side.

If you require additional validation of route ownership across ExpressRoute public peering, you can check the advertised routes against the list of all IPv4 and IPv6 IP prefixes that represent [Microsoft's public IP ranges](#). These ranges cover the full Microsoft address space and change infrequently, providing a reliable set of ranges to filter against that also provides additional protection to customers who are concerned about non-Microsoft owned routes leaking into their environment. In the event there's a change, it will be made on the 1st of the month and the version number in the **details** section of the page will change every time the file is updated.

There are many reasons to avoid the use of the [Office 365 URLs and IP address ranges](#) for generating prefix filter lists. Including the following:

- The Office 365 IP prefixes undergo lots of changes on a frequent basis.
- The Office 365 URLs and IP address ranges are designed for managing firewall allow lists and Proxy infrastructure, not routing.
- The Office 365 URLs and IP address ranges don't cover other Microsoft services that may be in scope for your ExpressRoute connections.

OPTION	COMPLEXITY	CHANGE CONTROL
Accept all Microsoft routes	Low: Customer relies upon Microsoft controls to ensure all routes are properly owned.	None

OPTION	COMPLEXITY	CHANGE CONTROL
Filter Microsoft owned supernets	Medium: Customer implements summarized prefix filter lists to allow only Microsoft owned routes.	Customers must ensure the infrequent updates are reflected in route filters.
Filter Office 365 IP ranges [!CAUTION] Not-Recommended	High: Customer filters routes based on defined Office 365 IP prefixes.	Customers must implement a robust change management process for the monthly updates. [!CAUTION] This solution requires significant on-going changes. Changes not implemented in time will likely result in a service outage.

Connecting to Office 365 using Azure ExpressRoute is based on BGP advertisements of specific IP subnets that represent networks where Office 365 endpoints are deployed. Due to the global nature of Office 365 and the number of services that make up Office 365, customers often have a need to manage the advertisements they accept on their network. If you're concerned with number of prefixes advertised into your environment, the [BGP community](#) feature allows you to filter the advertisements to a specific set of Office 365 services. This feature is now in preview.

Regardless of how you manage the BGP route advertisements coming from Microsoft, you won't gain any special exposure to Office 365 services when compared to connecting to Office 365 over an internet circuit alone. Microsoft maintains the same security, compliance, and performance levels regardless of the type of circuit a customer uses to connect to Office 365.

Security

Microsoft recommends that you maintain your own network and security perimeter controls for connections going to and from ExpressRoute public and Microsoft peering, which includes connections to and from Office 365 services. Security controls should be in place for network requests that travel outbound from your network to Microsoft's network and inbound from Microsoft's network to your network.

Outbound from Customer to Microsoft

When computers connect to Office 365, they connect to the same set of endpoints regardless of whether the connection is made over an internet or ExpressRoute circuit. Regardless of the circuit being used, Microsoft recommends that you treat Office 365 services as more trusted than generic internet destinations. Your outbound security controls should focus on the ports and protocols to reduce exposure and minimize ongoing maintenance. The required port information is available in the [Office 365 endpoints](#) reference article.

For added controls, you can use FQDN level filtering within your proxy infrastructure to restrict or inspect some or all network requests destined for the internet or Office 365. Maintaining the list of FQDNs as features are released and the Office 365 offerings evolve requires more robust change management and tracking of changes to the published [Office 365 endpoints](#).

Caution

Microsoft recommends you don't rely solely on IP prefixes to manage outbound security to Office 365.

OPTION	COMPLEXITY	CHANGE CONTROL
No restrictions	Low: Customer allows unrestricted outbound access to Microsoft.	None
Port restrictions	Low: Customer restricts outbound access to Microsoft by the expected ports.	Infrequent.

OPTION	COMPLEXITY	CHANGE CONTROL
FQDN restrictions	High: Customer restricts outbound access to Office 365 based on the published FQDNs.	Monthly changes.

Inbound from Microsoft to Customer

There are several optional scenarios that require Microsoft to initiate connections to your network.

- ADFS during password validation for sign in.
- [Exchange Server Hybrid deployments](#).
- Mail from an Exchange Online tenant to an on-premises host.
- SharePoint Online Mail sent from SharePoint Online to an on-premises host.
- [SharePoint federated hybrid search](#).
- [SharePoint hybrid BCS](#).
- [Skype for Business hybrid](#) and/or [Skype for Business federation](#).
- [Skype for Business Cloud Connector](#).

Microsoft recommends that you accept these connections over your internet circuit instead of your ExpressRoute circuit to reduce complexity. If your compliance or performance needs dictate these inbound connections must be accepted over an ExpressRoute circuit, using a firewall or reverse proxy to scope the accepted connections is recommended. You can use the [Office 365 endpoints](#) to figure out the right FQDNs and IP prefixes.

Compliance

We don't rely on the routing path you use for any of our compliance controls. Regardless of whether you connect to Office 365 services over an ExpressRoute or internet circuit, our compliance controls won't change. You should review the different compliance and security certification levels for Office 365 to figure out the best choice for meeting your organization's needs.

Here's a short link you can use to come back: <https://aka.ms/manageexpressroute365>

Related topics

[Content delivery networks](#)

[Office 365 URLs and IP address ranges](#)

[Managing Office 365 endpoints](#)

[Azure ExpressRoute for Office 365 Training](#)

Microsoft 365 Networking Partner Program

10/28/2022 • 2 minutes to read • [Edit Online](#)

Network connectivity has a direct impact on your users' ability to work quickly, collaborate effectively, and streamline business processes with Microsoft 365. For customers in any stage of their digital transformation, network design is a critical aspect that should be proactively addressed before issues negatively impact user experience.

As customers adopt Microsoft 365 for business productivity, Microsoft has observed a common trend that network performance and the resulting end-user collaboration experience is directly influenced by network solutions in the path between the user and Microsoft 365. To help partners design optimal network solutions and help customers make informed decisions regarding such solutions, we built the Microsoft 365 Networking Partner Program.

The Microsoft 365 Networking Partner Program deepens our collaboration with network partners and identifies key products and solutions that follow Microsoft 365 networking requirements, recommendations, and best practices. The goal of the Microsoft 365 Networking Partner program is to facilitate customer ability to improve their Microsoft 365 experience through easy discovery of validated partner solutions that consistently demonstrate alignment to key principles for optimal Microsoft 365 connectivity in customer deployments.

To modernize enterprise networks for great connectivity to Microsoft 365, customers often rely on network solution providers, on-premises or cloud-based security services, and system integrators to plan, design, and implement network connectivity for cloud services. Customers often ask Microsoft whether their network architecture and solutions work with Microsoft 365 and whether they align with Microsoft's [Network Connectivity Principles for Microsoft 365](#).

The Microsoft 365 Networking Partner Program helps answer these questions and demonstrates Microsoft's commitment to help our customers build and optimize their network architecture for the best Microsoft 365 experience. The Microsoft 365 team is working with many network industry partners to help ensure that the key principles for optimal connectivity are natively built into their network product and solutions.

The Microsoft 365 Networking Partner Program designates qualified networking solutions as "Works with Microsoft 365". Only devices or solutions that meet Microsoft's rigorous testing requirements, have seamless experiences with setup, and demonstrate a high-quality networking experience when used with Microsoft 365 will receive the "Works with Microsoft 365" designation. These validated partner solutions are listed on the [Microsoft 365 networking partners page](#), along with solution details and links to learn more.

Tenant roadmap for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

Your Microsoft 365 tenant is the set of services assigned to your organization. Typically, this tenant is associated with one or more of your public DNS domain names and acts as a central and isolated container for different subscriptions and the licenses within them that you assign to user accounts. For more information, see [Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings](#).

When you create a Microsoft 365 tenant, you assign it to a specific geographical location. You can also have a tenant with multiple geographical locations and move your tenant from one location to another.

To get your tenant ready for user, groups, licenses, and cloud apps, it's critical to carefully plan and execute your tenant configuration.

Set up your Microsoft 365 tenant

After ensuring that your networking is optimized for access to Microsoft 365 for both on-premises and remote workers, your next big tasks are planning for and then configuring your Microsoft 365 tenant for DNS domain names, common services, and for that identity infrastructure that supports secure user sign-in.

Plan

To plan for your tenant implementation:

- [Understand subscriptions, licenses, and Azure Active Directory \(Azure AD\) tenants](#)
- [Understand how to use third-party SSL certificates](#)
- [Understand the ways a Microsoft 365 tenant is integrated with Azure AD services](#)
- [Plan for client app support](#)
- [Determine how to use hybrid modern authentication](#)
- [Plan for Office 2007 and Office 2010 upgrades](#)
- [Understand tenant isolation](#)

Deploy

To deploy your tenant:

- Add the [DNS domains](#) for your organization.
- Use the [setup guides in the Microsoft 365 admin center](#).
- Build out your [identity infrastructure](#).

Move a tenant's geographic locations

Microsoft continues to open new datacenter geographic locations (geos) for Microsoft 365 services. These new datacenter geos add capacity and compute resources to support customer demand and usage growth. Additionally, the new datacenter geos offer in-geo data residency for core customer data.

For more information, see [Moving core data to new Microsoft 365 datacenter geos](#).

Deploy Microsoft 365 Multi-Geo

With Microsoft 365 Multi-Geo, your organization can expand its Microsoft 365 presence to multiple geographic regions and/or countries within your existing tenant.

For more information, see [Microsoft 365 Multi-Geo](#).

Manage multiple Microsoft 365 tenants

Although having a single tenant for your organization is ideal, you may be one of many organizations that have multiple tenants. Reasons can include mergers and acquisitions, you want administrative isolation, or you have a decentralized IT.

If you have multiple Microsoft 365 tenants, see these articles for more information about:

- [Inter-tenant collaboration](#)
- [Cross-tenant mailbox migration](#)
- [Tenant-to-tenant migrations](#)

Next step

Start your tenant planning with [Subscriptions, licenses, accounts, and tenants](#).

Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings

10/28/2022 • 6 minutes to read • [Edit Online](#)

Microsoft provides a hierarchy of organizations, subscriptions, licenses, and user accounts for consistent use of identities and billing across its cloud offerings:

- Microsoft 365 and Microsoft Office 365
- Microsoft Azure
- Microsoft Dynamics 365

Elements of the hierarchy

Here are the elements of the hierarchy:

Organization

An organization represents a business entity that is using Microsoft cloud offerings, typically identified by one or more public Domain Name System (DNS) domain names, such as contoso.com. The organization is a container for subscriptions.

Subscriptions

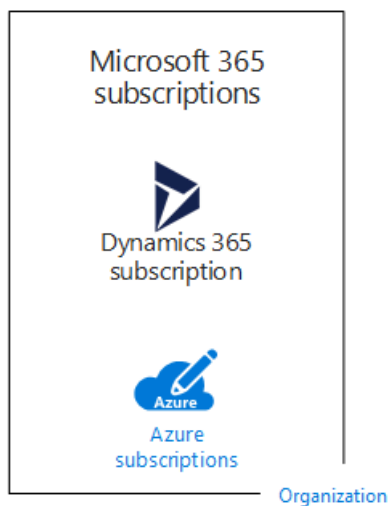
A subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based on either a per-user license fee or on cloud-based resource consumption.

- Microsoft's Software as a Service (SaaS)-based cloud offerings (Microsoft 365 and Dynamics 365) charge per-user license fees.
- Microsoft's Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud offerings (Azure) charge based on cloud resource consumption.

You can also use a trial subscription, but the subscription expires after a specific amount of time or consumption charges. You can convert a trial subscription to a paid subscription.

Organizations can have multiple subscriptions for Microsoft's cloud offerings. Figure 1 shows a single organization that has multiple Microsoft 365 subscriptions, a Dynamics 365 subscription, and multiple Azure subscriptions.

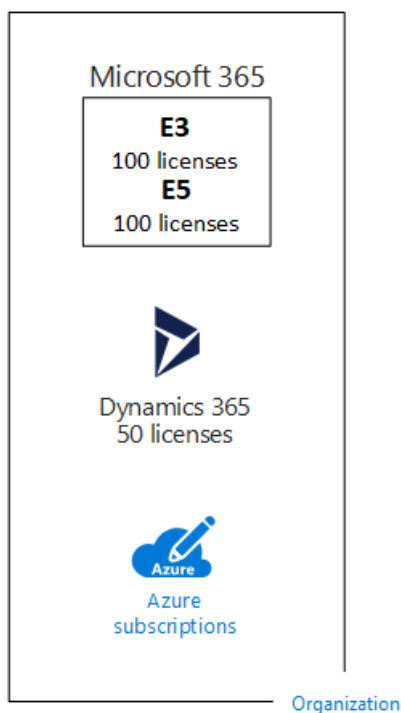
Figure 1: Example of multiple subscriptions for an organization



Licenses

For Microsoft's SaaS cloud offerings, a license allows a specific user account to use the services of the cloud offering. You are charged a fixed monthly fee as part of your subscription. Administrators assign licenses to individual user accounts in the subscription. For the example in Figure 2, the Contoso Corporation has a Microsoft 365 E5 subscription with 100 licenses, which allows to up to 100 individual user accounts to use Microsoft 365 E5 features and services.

Figure 2: Licenses within the SaaS-based subscriptions for an organization



NOTE

A security best practice is to use separate user accounts that are assigned specific roles for administrative functions. These dedicated administrator accounts do not need to be assigned a license for the cloud services that they administer. For example, a SharePoint administrator account does not need to be assigned a Microsoft 365 license.

For Azure PaaS-based cloud services, software licenses are built into the service pricing.

For Azure IaaS-based virtual machines, additional licenses to use the software or application installed on a virtual machine image might be required. Some virtual machine images have licensed versions of software installed and the cost is included in the per-minute rate for the server. Examples are the virtual machine images

for SQL Server 2014 and SQL Server 2016.

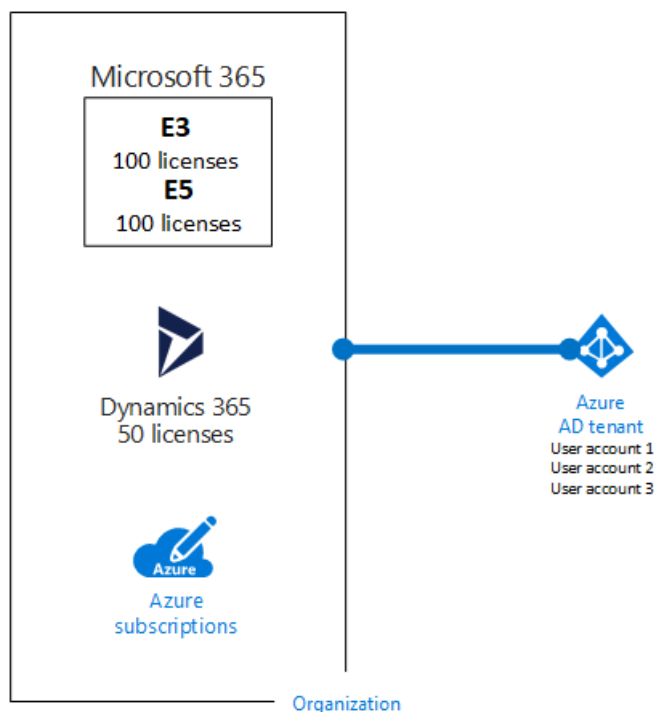
Some virtual machine images have trial versions of applications installed and need additional software application licenses for use beyond the trial period. For example, the SharePoint Server 2016 Trial virtual machine image includes a trial version of SharePoint Server 2016 pre-installed. To continue using SharePoint Server 2016 after the trial expiration date, you must purchase a SharePoint Server 2016 license and client licenses from Microsoft. These charges are separate from the Azure subscription and the per-minute rate to run the virtual machine still applies.

User accounts

User accounts for all of Microsoft's cloud offerings are stored in an Azure Active Directory (Azure AD) tenant, which contains user accounts and groups. An Azure AD tenant can be synchronized with your existing Active Directory Domain Services (AD DS) accounts using Azure AD Connect, a Windows server-based service. This is known as directory synchronization.

Figure 3 shows an example of multiple subscriptions of an organization using a common Azure AD tenant that contains the organization's accounts.

Figure 3: Multiple subscriptions of an organization that use the same Azure AD tenant



Tenants

For SaaS cloud offerings, the tenant is the regional location that houses the servers providing cloud services. For example, the Contoso Corporation chose the European region to host its Microsoft 365, EMS, and Dynamics 365 subscriptions for the 15,000 workers in their Paris headquarters.

Azure PaaS services and virtual machine-based workloads hosted in Azure IaaS can have tenancy in any Azure datacenter across the world. You specify the Azure datacenter, known as the location, when you create the Azure PaaS app or service or element of an IaaS workload.

An Azure AD tenant is a specific instance of Azure AD containing accounts and groups. Paid or trial subscriptions of Microsoft 365 or Dynamics 365 include a free Azure AD tenant. This Azure AD tenant does not include other Azure services and is not the same as an Azure trial or paid subscription.

Summary of the hierarchy

Here is a quick recap:

- An organization can have multiple subscriptions
 - A subscription can have multiple licenses
 - Licenses can be assigned to individual user accounts
 - User accounts are stored in an Azure AD tenant

Here is an example of the relationship of organizations, subscriptions, licenses, and user accounts:

- An organization identified by its public domain name.
 - A Microsoft 365 E3 subscription with user licenses.
 - A Microsoft 365 E5 subscription with user licenses.
 - A Dynamics 365 subscription with user licenses.

Multiple Azure subscriptions.

- The organization's user accounts in a common Azure AD tenant.

Multiple Microsoft cloud offering subscriptions can use the same Azure AD tenant that acts as a common identity provider. A central Azure AD tenant that contains the synchronized accounts of your on-premises AD DS provides cloud-based Identity as a Service (IDaaS) for your organization.

Figure 4: Synchronized on-premises accounts and IDaaS for an organization

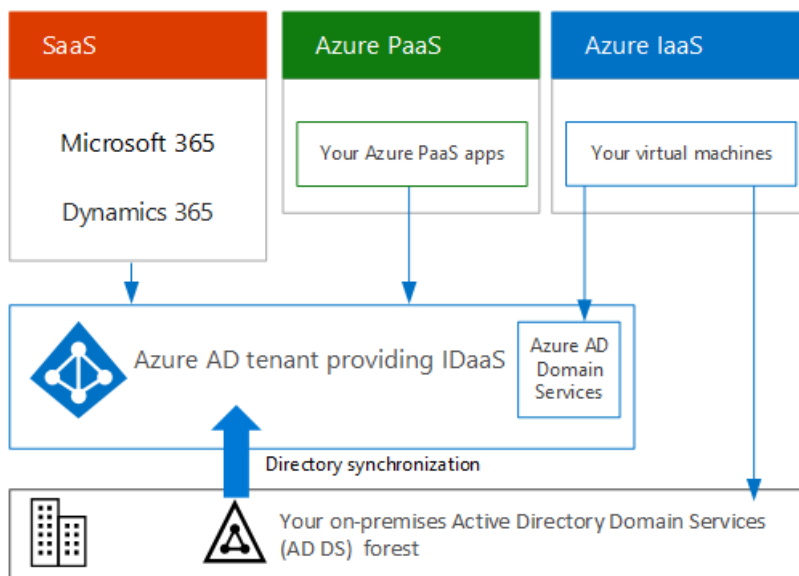


Figure 4 shows how a common Azure AD tenant is used by Microsoft's SaaS cloud offerings, Azure PaaS apps, and virtual machines in Azure IaaS that use Azure AD Domain Services. Azure AD Connect synchronizes the on-premises AD DS forest with the Azure AD tenant.

Combining subscriptions for multiple Microsoft cloud offerings

The following table describes how you can combine multiple Microsoft cloud offerings based on already having a subscription for one type of cloud offering (the labels going down the first column) and adding a subscription for a different cloud offering (going across the columns).

	MICROSOFT 365	AZURE	DYNAMICS 365
--	---------------	-------	--------------

	MICROSOFT 365	AZURE	DYNAMICS 365
Microsoft 365	NA	You add an Azure subscription to your organization from the Azure portal.	You add a Dynamics 365 subscription to your organization from the Microsoft 365 admin center.
Azure	You add a Microsoft 365 subscription to your organization.	NA	You add a Dynamics 365 subscription to your organization.
Dynamics 365	You add a Microsoft 365 subscription to your organization.	You add an Azure subscription to your organization from the Azure portal.	NA

An easy way to add subscriptions to your organization for Microsoft SaaS-based services is through the admin center:

1. Sign in to the Microsoft 365 admin center (<https://admin.microsoft.com>) with your **User Admin**, or **Global admin** account.
2. From the left navigation of the **Admin center** home page, click **Billing**, and then **Purchase services**.
3. On the **Purchase services** page, purchase your new subscriptions.

The admin center assigns the organization and Azure AD tenant of your Microsoft 365 subscription to the new subscriptions for SaaS-based cloud offerings.

To add an Azure subscription with the same organization and Azure AD tenant as your Microsoft 365 subscription:

1. Sign in to the Azure portal (<https://portal.azure.com>) with your Microsoft 365 **Azure AD DC admin**, or **Global admin** account.
2. In the left navigation, click **Subscriptions**, and then click **Add**.
3. On the **Add subscription** page, select an offer and complete the payment information and agreement.

If you purchased Azure and Microsoft 365 subscriptions separately and want to access the Microsoft 365 Azure AD tenant from your Azure subscription, see the instructions in [Add an existing Azure subscription to your Azure Active Directory tenant](#).

See also

[Microsoft cloud for enterprise architects illustrations](#)

[Architectural models for SharePoint, Exchange, Skype for Business, and Lync](#)

[Hybrid solutions](#)

Next step

[Assessing Microsoft 365 network connectivity](#)

Plan for third-party SSL certificates for Microsoft 365

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

To encrypt communications between your clients and the Microsoft 365 environment, third-party Secure Socket Layer (SSL) certificates must be installed on your infrastructure servers.

This article is part of [Network planning and performance tuning for Microsoft 365](#).

Certificates are required for the following Microsoft 365 components:

- Exchange on-premises
- Single sign-on (SSO) (for both the Active Directory Federation Services (AD FS) federation servers and AD FS federation server proxies)
- Exchange Online services, such as Autodiscover, Outlook Anywhere, and Exchange Web Services
- Exchange hybrid server

Certificates for Exchange On-Premises

For an overview about how to use digital certificates to make the communication between the on-premises Exchange organization and Exchange Online secure, see the TechNet article [Understanding Certificate Requirements](#).

Certificates for Single Sign-On

To provide your users with a simplified single sign-on experience that includes robust security, the certificates shown in the following table are required on either the federation servers or the federation server proxies. The table below focuses on Active Directory Federation Services (AD FS), we also have more information on [using third-party identity providers](#).

CERTIFICATE TYPE	DESCRIPTION	WHAT YOU NEED TO KNOW BEFORE YOU DEPLOY
------------------	-------------	---

CERTIFICATE TYPE	DESCRIPTION	WHAT YOU NEED TO KNOW BEFORE YOU DEPLOY
SSL certificate (also called a server authentication certificate)	This is a standard SSL certificate that is used to make communications between federation servers, clients, and federation server proxy computers secure.	AD FS requires an SSL certificate. By default, AD FS uses the SSL certificate that is configured for the default website in Internet Information Services (IIS). The subject name of this SSL certificate is used to determine the Federation Service (FS) name for each instance of AD FS that you deploy. Consider choosing a subject name for any new certification authority (CA)-issued certificates that best represents the name of your company or organization to Microsoft 365. This name must be Internet-routable. Caution: AD FS requires that this SSL certificate have no dotless (short-name) subject name. Recommendation: Because this certificate must be trusted by clients of AD FS, we recommend that you use an SSL certificate issued by a public (third-party) CA or by a CA that is subordinate to a publicly trusted root; for example, VeriSign or Thawte.
Token-signing certificate	This is a standard X.509 certificate that's used for securely signing all tokens that the federation server issues and that Microsoft 365 accepts and validates.	The token-signing certificate must contain a private key that chains to a trusted root in the FS. By default, AD FS creates a self-signed certificate. However, depending on the needs of your organization, you can change this certificate to a CA-issued certificate by using the AD FS management snap-in. Caution: The token-signing certificate is critical to the stability of the FS. If the certificate is changed, Microsoft 365 must be notified of the change. If notification is not provided, users can't sign in to their Microsoft 365 service offerings. Recommendation: We recommend that you use the self-signed token-signing certificate that is generated by AD FS. By doing so, it manages this certificate for you by default. For example, when this certificate is about to expire, AD FS will generate a new self-signed certificate.

Federation server proxies require the certificate that is described in the following table.

CERTIFICATE TYPE	DESCRIPTION	WHAT YOU NEED TO KNOW BEFORE YOU DEPLOY
------------------	-------------	---

CERTIFICATE TYPE	DESCRIPTION	WHAT YOU NEED TO KNOW BEFORE YOU DEPLOY
SSL certificate	This is a standard SSL certificate that is used for securing communications between a federation server, a federation server proxy, and Internet client computers.	This SSL certificate must be bound to the default website in IIS before you can successfully run the AD FS Federation Server Proxy Configuration wizard. This certificate must have the same subject name as the SSL certificate that was configured on the federation server in the corporate network. Recommendation: We recommend that you use the same server authentication certificate that is configured on the federation server that this federation server proxy connects to.

Certificates for Autodiscover, Outlook Anywhere, and Active Directory Synchronization

Your external-facing Exchange 2013, Exchange 2010, Exchange 2007, and Exchange 2003 Client Access servers (CASs) require a third-party SSL certificate for secure connections for Autodiscover, Outlook Anywhere, and Active Directory synchronization services. You may already have this certificate installed in your on-premises environment.

Certificate for an Exchange Hybrid Server

Your external-facing Exchange hybrid server or servers require a third-party SSL certificate for secure connectivity with the Exchange Online service. You need to get this certificate from your third-party SSL provider.

Microsoft 365 Certificate Chains

This article describes the certificates you may need to install on your infrastructure. For more information on the certificates installed on our Microsoft 365 servers, see [Microsoft 365 Certificate Chains](#).

See also

[Microsoft 365 Enterprise overview](#)

Setup guides for Microsoft 365 and Office 365 services

10/28/2022 • 16 minutes to read • [Edit Online](#)

Microsoft 365 and Office 365 setup guides give you tailored guidance and resources for planning and deploying your tenant, apps, and services. These guides are created using the same best practices that [Microsoft 365 FastTrack](#) onboarding specialists share in individual interactions, and they're available to all admins within the Microsoft 365 admin center. They give information on product setup, enabling security features, deploying collaboration tools, and provide scripts to speed up advanced deployments.

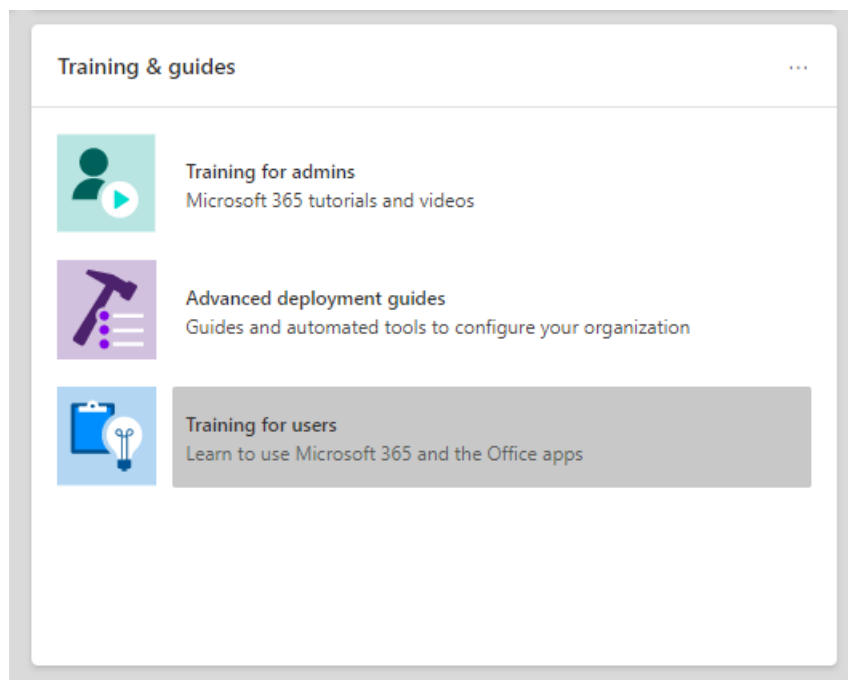
NOTE

You must be assigned an admin role like Global Reader to access the Microsoft 365 setup guides. Only admins with the Global Administrator role can use the guides to change settings in the tenant.

How to access setup guides in the Microsoft 365 admin center

The setup guides are accessible from the [Setup guidance](#) page in the Microsoft 365 admin center. You can keep track of the status of your progress and return at any time to complete a guide. To reach the **Setup guidance** page:

1. In the [Microsoft 365 admin center](#), go to the **Home** page.
2. Find the **Training & guides** card.



3. Select **Advanced deployment guides** and then select **All guides**.

Microsoft 365 admin center

Search

Home

Users

Active users

Contacts

Guest users

Deleted users

Devices

Teams & groups

Roles

Resources

Billing

Support

Settings

Setup

Reports

Health

Admin centers

Security

Compliance

Endpoint Manager

Azure Active Directo...

Home > Advanced deployment guides

Advanced deployment guides

Overview All guides Training resources Request assistance

Here are all guides sorted by category. Use the filter or search to find a specific guide to deploy services and features to your environment.

Completed0

In progress0

Not started40

Filters:

Category: All

Product: All

Status: All

Name	Services
Initial setup	
Prepare your environment	Office Exchange
Email setup guide	Exchange
Migrate Gmail contacts and calendar items	Exchange
Microsoft 365 setup guide	Windows 10

Guides for initial setup

Prepare your environment

The [Prepare your environment](#) guide helps you prepare your organization's environment for Microsoft 365 and Office 365 services. Whatever your goals are, there are tasks you'll need to complete to ensure a successful deployment. To avoid any errors while preparing your environment, you're provided with step-by-step instructions to connect your domain, add users, assign licenses, set up email with Exchange Online, and install or deploy Office apps.

Email setup guide

The [Email setup guide](#) provides you with the step-by-step guidance needed for configuring Exchange Online for your organization. This guidance includes setting up new email accounts, migrating email, and configuring email protection. For a successful email setup, use this advisor and you'll receive the recommended migration method based on your organization's current mail system, the number of mailboxes being migrated, and how you want to manage users and their access.

Migrate Gmail contacts and calendar items

When you migrate a Gmail user's mailbox to Microsoft 365, email messages are migrated, but contacts and calendar items are not. The [Gmail contacts and calendar advisor](#) provides steps for importing Google contacts and Google calendar items to Microsoft 365 using import and export methods with Outlook.com, the Outlook client, or PowerShell.

Microsoft 365 setup guide

The [Microsoft 365 setup guide](#) provides you with guidance when setting up productivity tools, security policies, and device management capabilities. With a Microsoft 365 Business Premium or Microsoft 365 for enterprise subscription, you can use this advisor to set up and configure your organization's devices.

You'll receive guidance and access to resources to enable your cloud services, update devices to the latest supported version of Windows 10, and join devices to Azure Active Directory (Azure AD), all in one central location.

Remote work setup guide

The [Remote work setup guide](#) provides organizations with the tips and resources needed to ensure your users can successfully work remotely, your data is secure, and users' credentials are safeguarded.

You'll receive guidance to optimize remote workers' device traffic to both Microsoft 365 resources in the cloud and your organization's network, which will reduce the strain on your remote access VPN infrastructure.

Microsoft Edge setup guide

Microsoft Edge has been rebuilt from the ground up to bring you world-class compatibility and performance, the security and privacy you deserve, and new features designed to bring you the best of the web.

The [Microsoft Edge setup guide](#) will help you configure Enterprise Site Discovery to see which sites accessed in your org might need to use IE mode, review and configure important security features, configure privacy policies and compliance policies to meet your org's requirements, and manage web access on your devices. You can download Microsoft Edge to individual devices, or we'll show you how to deploy to multiple users in your org with Group Policy, Configuration Manager, or Microsoft Intune.

Configure IE mode for Microsoft Edge

If you've already deployed Microsoft Edge and only want to configure IE mode, the [Configure IE mode for Microsoft Edge guide](#) will give you scripts to automate the configuration of Enterprise Site Discovery. You'll also get IE mode recommendations from a cloud-based tool that will help you create an Enterprise Mode Site List to deploy to your users.

Microsoft Search setup guide

Microsoft Search helps your organization find what they need to complete what they're working on. Whether it's searching for people, files, org charts, sites, or answers to common questions, your org can use Microsoft Search throughout their workday to get answers.

The [Microsoft Search setup guide](#) helps you configure Microsoft Search whether you want to pilot it to a group of users or roll it out to everyone in your org. You'll assign Search admins and Search editors and then customize the search experience for your users with answers and more options, like adding the Bing extension to Chrome or setting Bing as your default search engine.

Block use of Internet Explorer in your organization

Microsoft support for Internet Explorer 11 is ending soon for most versions of Windows 10. The [Block use of Internet Explorer in your organization guide](#) ensures that your users can still run legacy web apps that rely on Internet Explorer. This guide also helps you move those users to Microsoft Edge with IE mode.

Guides for authentication and access

Configure multi-factor authentication (MFA)

The [Configure multi-factor authentication \(MFA\) guide](#) provides information to secure your organization against breaches due to lost or stolen credentials. MFA immediately increases account security by prompting for multiple forms of verification to prove a user's identity when they sign in to an app or other company resource. This prompt could be to enter a code on the user's mobile device or to provide a fingerprint scan. MFA is enabled through Conditional Access, security defaults, or per-user MFA. This guide will provide the recommended MFA option for your org, based on your licenses and existing configuration.

Identity security for Teams

The [Identity security for teams guide](#) helps you with some basic security steps you can take to ensure your users are safe and have the most productive time using Teams.

Add or sync users to Microsoft 365

[This guide](#) will help streamline the process of getting your user accounts set up in **Microsoft 365**. Based on your environment and needs, you can choose to add users individually, migrate your on-premises directory with Azure AD cloud sync or Azure AD Connect, or troubleshoot existing sync problems when necessary.

Azure AD setup guide

The [Azure AD setup guide](#) provides information to ensure your organization has a strong security foundation. In this guide you'll set up initial features, like Azure Role-based access control (Azure RBAC) for admins, Azure AD Connect for your on-premises directory, and Azure AD Connect Health, so you can monitor your hybrid identity's health during automated syncs.

It also includes essential information on enabling self-service password resets, conditional access and integrated third party sign-on including optional advanced identity protection and user provisioning automation.

Sync users from your Windows Server Active Directory

The [Sync users from your Windows Server Active Directory](#) guide walks you through turning on directory synchronization. Directory synchronization brings your on-premises and cloud identities together for easier access and simplified management. Unlock new capabilities, like single sign-on, self-service options, automatic account provisioning, conditional access controls, and compliance policies. These capabilities ensure your users have access to the resources they need from anywhere.

Plan your passwordless deployment

Upgrade to an alternative sign-in approach that allows users to access their devices securely with one of the following passwordless authentication methods:

- Windows Hello for Business
- The Microsoft Authenticator app
- Security keys

Use the [Plan your passwordless deployment](#) guide to discover the best passwordless authentication methods to use and receive guidance on how to deploy them.

Integrate a third-party cloud app with Azure AD

[This guide](#) helps IT admins to select and configure the App.

Plan your self-service password reset (SSPR) deployment

Give users the ability to change or reset their password independently, if their account is locked, or they forget their password without the need to contact a helpdesk engineer.

Use the [Plan your self-service password reset deployment](#) guide to receive relevant articles and instructions for configuring the appropriate Azure portal options to help you deploy SSPR in your environment.

Guides for security and compliance

Security analyzer

The [Security analyzer](#) will analyze your security approach and introduce you to Microsoft integrated security and compliance solutions that can improve your security posture. You'll learn about advanced features, such as managing identities and helping to protect against modern attacks. You can then sign up for a trial subscription and be pointed to the corresponding setup guidance for each solution.

Microsoft Intune setup guide

Set up Microsoft Intune to manage devices in your organization. For full control of corporate devices, you'll use Intune's mobile device management (MDM) features. To manage your organization's data on shared and personal devices, you can use Intune's mobile application management (MAM) features.

With the [Microsoft Intune setup guide](#), you'll set up device and app compliance policies, assign app protection policies, and monitor the device and app protection status.

Microsoft Defender for Endpoint setup guide

The [Microsoft Defender for Endpoint setup guide](#) provides instructions that will help your enterprise network prevent, detect, investigate, and respond to advanced threats. Make an informed assessment of your organization's vulnerability and decide which deployment package and configuration methods are best.

NOTE

A Microsoft Volume License is required for Microsoft Defender for Endpoint.

Exchange Online Protection setup guide

Microsoft Exchange Online Protection (EOP) is a cloud-based email filtering service for protection against spam and malware, with features to safeguard your organization from messaging policy violations.

Use the [Exchange Online Protection setup guide](#) to set up EOP by selecting which of the three deployment scenarios—on-premises mailboxes, hybrid (mix of on-premises and cloud) mailboxes, or all cloud mailboxes—fits your organization. The guide provides information and resources to set up and review your user's licensing, assign permissions in the Microsoft 365 admin center, and configure your organization's anti-malware and spam policies in the Security & Compliance Center.

Microsoft Defender for Office 365 setup guide

The [Microsoft Defender for Office 365 setup guide](#) safeguards your organization against malicious threats that your environment might come across through email messages, links, and third party collaboration tools. This guide provides you with the resources and information to help you prepare and identify the Defender for Office 365 plan to fit your organization's needs.

Microsoft Defender for Identity setup guide

The [Microsoft Defender for Identity setup guide](#) provides security solution set-up guidance to identify, detect, and investigate advanced threats that might compromise user identities. These include detecting suspicious user activities and malicious insider actions directed at your organization. You'll create a Defender for Identity instance, connect to your organization's Active Directory, and then set up sensors, alerts, notifications, and configure your unique portal preferences.

Insider risk solutions setup guide

The [Insider risk solutions setup guide](#) helps you protect your organization against insider risks that can be challenging to identify and difficult to mitigate. Insider risks occur in a variety of areas and can cause major problems for organizations, ranging from the loss of intellectual property to workplace harassment, and more.

The solutions in this guide will help you gain visibility into user activities, actions, and communications with native signals and enrichments from across your organization:

- With the communication compliance solution, you can identify and act on communication risks for items like workplace violence, insider trading, harassment, code of conduct, and regulatory compliance violations.
- The insider risk management solution helps you identify, investigate, and take action on risks for intellectual property theft, sensitive data leaks, security violations, data spillage, and confidentiality violations.

Microsoft Purview Information Protection setup guide

Get an overview of the capabilities you can apply to your information protection strategy so you can be confident your sensitive information is protected. Use a four-stage lifecycle approach in which you discover, classify, protect, and monitor sensitive information. The [Microsoft Purview Information Protection setup guide](#) provides guidance for completing each of these stages.

Microsoft Purview Data Lifecycle Management setup guide

The [Microsoft Purview Data Lifecycle Management setup guide](#) provides you with the information you'll need to set up and manage your organization's governance strategy, to ensure that your data is classified and managed according to the specific lifecycle guidelines you set. With this guide, you'll learn how to create, auto-apply, or publish retention labels, retention label policies, and retention policies that are applied to your organization's content and compliance records. You'll also get information on importing CSV files with a file plan for bulk scenarios or for applying them manually to individual documents.

Microsoft Defender for Cloud Apps setup guide

The [Microsoft Defender for Cloud Apps setup guide](#) provides easy to follow deployment and management guidance to set up your Cloud Discovery solution. With Cloud Discovery, you'll integrate your supported security apps, and then you'll use traffic logs to dynamically discover and analyze the cloud apps that your organization uses. You'll also set up features available through the Defender for Cloud Apps solution, including threat detection policies to identify high-risk use, information protection policies to define access, and real-time session controls to monitor activity. With these features, your environment gets enhanced visibility, control over data movement, and analytics to identify and combat cyberthreats across all your Microsoft and third party cloud services.

Audit solutions setup guide

The [Microsoft 365 auditing solutions guide](#) provides an integrated solution to help organizations effectively respond to security events, forensic investigations, and compliance obligations. When you use the auditing solutions in Microsoft 365, you can search the audit log for activities performed in different Microsoft 365 services.

eDiscovery solutions setup guide

eDiscovery is the process of identifying and delivering electronic information that can be used as evidence in legal cases. The eDiscovery solutions setup guide assists in the use of eDiscovery tools in Microsoft Purview that allow you to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer communities.

Guides for collaboration

Build your employee experience

Transform how your employees work together with the [Employee experience dashboard](#). For seamless teamwork, use Microsoft 365 to create productive, aligned teams, and keep employees engaged with leadership and the rest of the organization. Help your employees be effective in all work activities. These guides will provide instructions on how to use SharePoint, Teams, and Yammer to build collaboration across your org to help drive productivity.

Microsoft 365 Apps setup guide

The [Microsoft 365 Apps setup guide](#) helps you get your users' devices running the latest version of Office products like Word, Excel, PowerPoint, and OneNote. You'll get guidance on the various deployment methods that include easy self-install options to enterprise deployments with management tools. The instructions will help you assess your environment, figure out your specific deployment requirements, and implement the necessary support tools to ensure a successful installation.

Mobile apps setup guide

The [Mobile apps setup guide](#) provides instructions for the download and installation of Office apps on your Windows, iOS, and Android mobile devices. This guide provides you with step-by-step information to download and install Microsoft 365 and Office 365 apps on your phone and tablet devices.

Microsoft Teams setup guide

The [Microsoft Teams setup guide](#) provides your organization with guidance to set up team workspaces that host

real-time conversations through messaging, calls, and audio or video meetings for both team and private communication. Use the tools in this guide to configure Guest access, set who can create teams, and add team members from a .csv file, all without the need to open a PowerShell session. You'll also get best practices for determining your organization's network requirements and ensuring a successful Teams deployment.

Teams Phone setup guide

The [Teams Phone setup guide](#) helps you stay connected with the use of modern calling solutions. Apply key capabilities with a cloud-based, call-control system that supports the telephony workload for Teams. You can choose and deploy features from the available public switched telephone network (PSTN) connectivity options. You can also find assistance for other features, such as auto attendant, call queues, Audio Conferencing, caller ID, and live events.

SharePoint setup guide

The [SharePoint setup guide](#) helps you set up your SharePoint document storage and content management, create sites, configure external sharing, migrate data and configure advanced settings, and drive user engagement and communication within your organization. You'll follow steps for configuring your content-sharing permission policies, choose your migration sync tools, and enable the security settings for your SharePoint environment.

OneDrive setup guide

Use the [OneDrive setup guide](#) to get started with OneDrive file storage, sharing, collaboration, and syncing capabilities. OneDrive provides a central location where users can sync their Microsoft 365 Apps files, configure external sharing, migrate user data, and configure advanced security and device access settings. The OneDrive setup guide can be deployed using a OneDrive subscription or a standalone OneDrive plan.

Yammer deployment advisor

Connect and engage across your organization with Yammer. The [Yammer deployment advisor](#) prepares your Yammer network by adding domains, defining admins, and combining Yammer networks. You'll get guidance to deploy Yammer and then customize the look, configure security and compliance, and refine the settings.

Advanced guides

In-place upgrade with Configuration Manager

Use the [In-place upgrade with Configuration Manager guide](#) when upgrading Windows 7 and Windows 8.1 devices to the latest version of Windows 10. You'll use the script provided to check the prerequisites and automatically configure an in-place upgrade.

Deploy Office to your users

Deploy Office apps from the cloud with the ability to customize your installation by using the Office Deployment Tool. The [Deploy Office to your users guide](#) helps you create a customized Office configuration with advanced settings, or you can use a pre-built recommended configuration. Whether your users are conducting a self-install or you're deploying to your users individually or in bulk, this advanced guide provides you with step-by-step instructions to give users an Office installation tailored to your organization.

Deploy Office to remote users

Now that working remotely is the norm, users need to receive your organization's Office settings when they're not connected to your internal network or when using their own devices.

Use the [Deploy Office to remote users guide](#) to create a customized Office installation and then send users a generated PowerShell script that will seamlessly install Office with your configuration.

Deploy and update Microsoft 365 Apps with Configuration Manager

For organizations using Configuration Manager, you can use the [Deploy and update Microsoft 365 Apps with Configuration Manager advisor](#) to generate a script that will automatically configure your Microsoft 365 Apps

deployment using best practices recommended by FastTrack engineers. Use this guide to build your deployment groups, customize your Office apps and features, configure dynamic or lean installations, and then run the script to create the applications, automatic deployment rules, and device collections you need to target your deployment.

Intune Configuration Manager co-management setup guide

Use the [Intune Configuration Manager co-management setup guide](#) to set up existing Configuration Manager client devices and new internet-based devices that your org wants to co-manage with both Microsoft Intune and Configuration Manager. Co-management allows you to manage Windows 10 devices and adds new functionality to your org's devices, while receiving the benefits of both solutions.

School Data Sync rollover setup guide

The [SDS Rollover setup guide](#) provides the steps to help your organization sync student information data to Azure Active Directory and Office 365. This guide streamlines the term lifecycle management process by creating Office 365 Groups for Exchange Online and SharePoint Online, class teams for Microsoft Teams and OneNote, as well as Intune for Education, and rostering and single sign-on integration for third-party apps. You'll perform end-of-year closeout, tenant cleanup and archive, new school year preparation, and new school year launch. Then you can create new profiles using the sync deployment method that suits your organization.

Integrated apps and Azure AD for Microsoft 365 administrators

10/28/2022 • 3 minutes to read • [Edit Online](#)

There's more to managing integrated apps than just [managing user consent to apps](#). With the advent of the Microsoft 365 REST APIs, users can grant apps access to their Microsoft 365 data, such as mail, calendars, contacts, users, groups, files, and folders. By default, users need to individually grant permissions to each app.

But this doesn't scale well if you want to authorize an app once at the **Azure AD DC admin**, or **Global admin** level and roll it out to your whole organization through the app launcher. To do this, you must register the app in Azure Active Directory (Azure AD). There are some steps you need to take before you can register an app in Azure AD and some background information you should know that can help you manage apps in your Microsoft 365 organization.

Azure AD resources for Microsoft 365 admins

You have to do these two tasks before you can manage your Microsoft 365 apps in Azure AD.

PREREQUISITES	COMMENTS
Use your free Azure AD subscription	Every paid subscription to Microsoft 365 comes with a free subscription to Azure AD. You can use Azure AD to manage your apps and to create and manage user and group accounts. To use Azure AD, just go to the Azure portal at https://portal.azure.com and sign in using your Microsoft 365 account.
Manage user consent to apps	You must manage user consent to apps to allow third-party apps to access user Microsoft 365 information and for you to register apps in Azure AD. For example, when someone uses a third-party app, that app might ask for permission to access their calendar and to edit files that are in a OneDrive folder.

Managing Microsoft 365 apps requires you to have knowledge of apps in Azure AD. Use these articles to give you the background you need.

ARTICLE	COMMENTS
Meet the Microsoft 365 app launcher	If you're new to the app launcher, you might be wondering what it is and how to use it. The app launcher is designed to help you get to your apps from anywhere in Microsoft 365.
Office 365 management APIs overview	The Microsoft 365 management APIs let you provide access to your Microsoft 365 data, including the things they care about most—their mail, calendars, contacts, users and groups, files, and folders.
Integrating applications in Azure AD	Learn about applications that are integrated with Azure AD, and how to register your application, understand concepts behind a registered application, and learn about branding guidelines for multi-tenant applications.

ARTICLE	COMMENTS
Add custom tiles to the app launcher	The app launcher in Microsoft 365 makes it easier for users to find and access their apps. This article describes the ways you as a developer can get your apps to appear in users' app launchers and also give them a single sign-on (SSO) experience using their Microsoft 365 credentials.
Azure AD integration tutorials	The objective of these tutorials is to show you how to configure Azure AD SSO for third-party SaaS applications.
Authentication scenarios for Azure AD	Azure AD simplifies authentication for developers by providing identity as a service, with support for industry-standard protocols such as OAuth 2.0 and OpenID Connect, as well as open source libraries for different platforms to help you quickly start coding. This document helps you understand the various scenarios Azure AD supports and shows you how to get started.
Application access	Azure AD enables easy integration to many of today's popular software as a service (SaaS) applications. It provides identity and access management, and it delivers an Access Panel for users where they can discover what application access they have and where they can use SSO to access their applications. This article provides you with links to the related resources that enable you to learn more about the application access enhancements for Azure AD and how you can contribute to them.
Personalize your Office 365 experience	You can get quick access to the apps you use every day by adding or removing apps in the Microsoft 365 app launcher.

Microsoft 365 integration with on-premises environments

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can integrate Microsoft 365 with your existing on-premises Active Directory Domain Services (AD DS) and with on-premises installations of Exchange Server, Skype for Business Server 2015, or SharePoint Server.

- When you integrate AD DS, you can synchronize and manage user accounts for both environments. You can also add password hash synchronization (PHS) or single sign-on (SSO) so users can log on to both environments with their on-premises credentials.
- When you integrate with on-premises server products, you create a hybrid environment. A hybrid environment can help as you migrate users or information to Microsoft 365, or you can continue to have some users or some information on-premises and some in the cloud. For more information about hybrid environments, see [hybrid cloud](#).

You can also use the Azure Active Directory (Azure AD) advisors for customized setup guidance in the Microsoft 365 admin center (you must be signed in to Microsoft 365):

- [Azure AD setup guide](#)
- [Sync users from your org's directory](#)
- [Active Directory Federation Services \(AD FS\) deployment advisor](#)

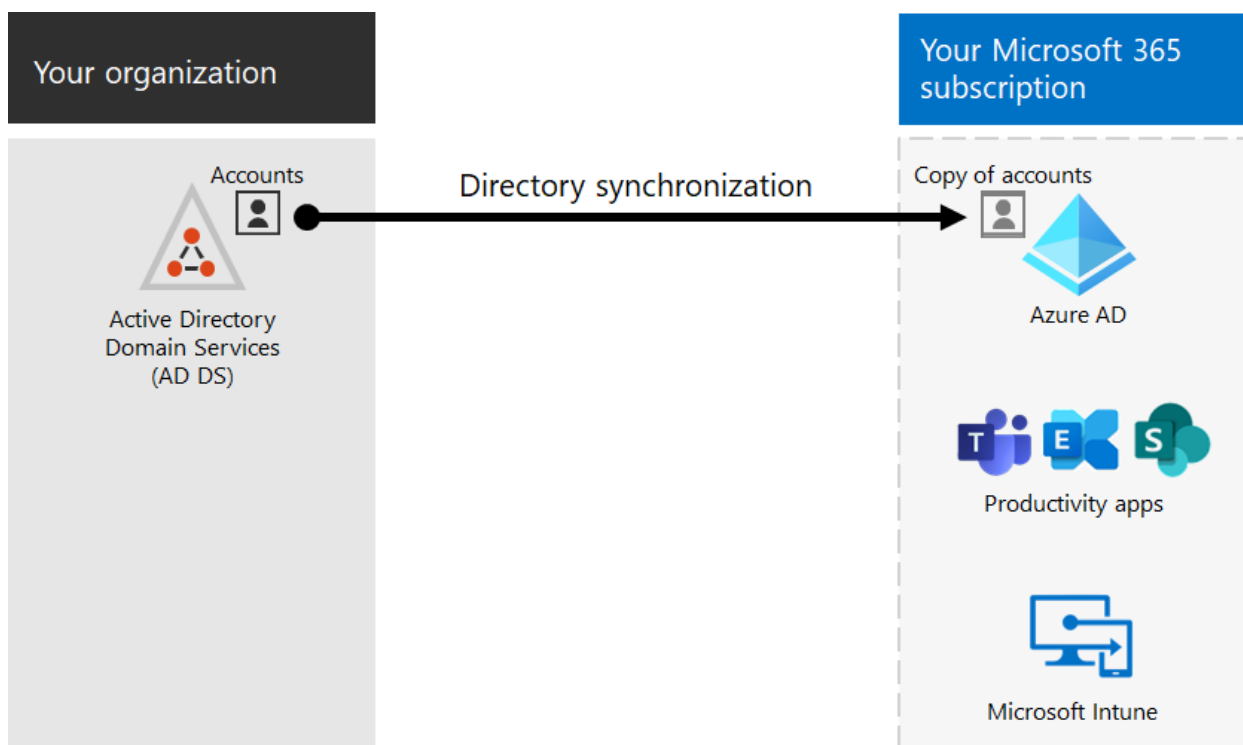
Before you begin

Before you integrate Microsoft 365 and an on-premises environment, you also need to do [network planning and performance tuning](#). You will also want to understand the available [identity models](#).

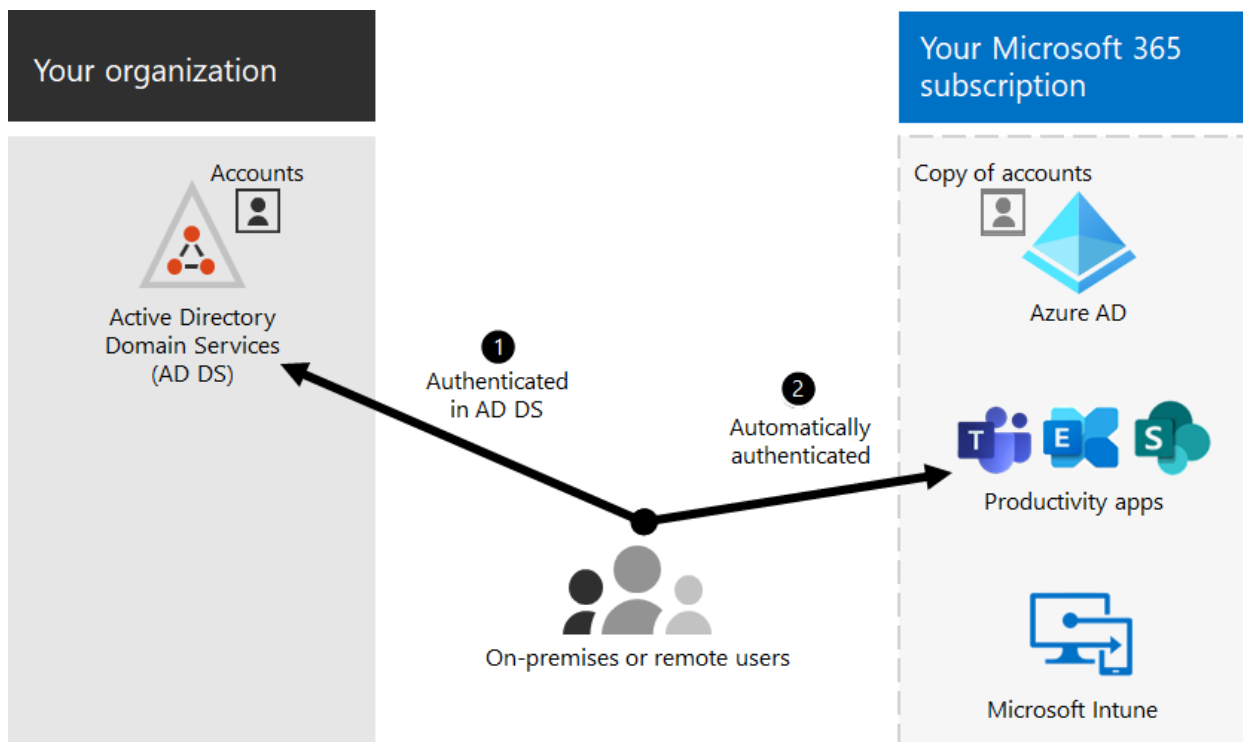
See [manage Microsoft 365 accounts](#) for a list of tools you can use to manage Microsoft 365 user accounts.

Integrate Microsoft 365 with AD DS

If you have existing user accounts in AD DS, you don't want to re-create all of those accounts in Microsoft 365 and risk introducing differences or errors between the environments. Directory synchronization helps you mirror those accounts between your on-premises and online environments. With directory synchronization, your users don't have to remember new information for each environment, and you don't have to create or update accounts twice. You will need to [prepare your on-premises directory](#) for directory synchronization.



If you want users to be able to log on to Microsoft 365 with their on-premises credentials, you can also configure SSO. With SSO, Microsoft 365 is configured to trust the on-premises environment for user authentication.



Directory synchronization with or without password hash synchronization or pass-through authentication (PTA)

A user logs on to their on-premises environment with their user account (domain\username). When they go to Microsoft 365, they must log on again with their work or school account (user@domain.com). The user name is the same in both environments. When you add PHS or PTA, the user has the same password for both environments, but will have to provide those credentials again when logging on to Microsoft 365. Directory synchronization with PHS is the most commonly used directory synchronization .

To set up directory synchronization, use Azure AD Connect. For instructions, see [Set up directory synchronization for Microsoft 365](#) and [Azure AD Connect with express settings](#).

Learn more about [preparing for directory synchronization to Microsoft 365](#).

Directory synchronization with SSO

A user logs on to their on-premises environment with their user account. When they go to Microsoft 365, they are either logged on automatically, or they log on using the same credentials they use for their on-premises environment (domain\username).

To set up SSO you also use Azure AD Connect. For instructions, see [Custom installation of Azure AD Connect](#).

For more information, see [single sign-on](#).

Azure AD Connect

Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync. If you want to update from Azure Active Directory Sync to Azure AD Connect, see [the upgrade instructions](#).

See also

[Microsoft 365 Enterprise overview](#)

Azure integration with Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 uses Azure Active Directory (Azure AD) to manage user identities behind the scenes. Your Microsoft 365 subscription includes a free Azure AD subscription so that you can integrate your on-premises Active Directory Domain Services (AD DS) to synchronize user accounts and passwords or set up single sign-on. You can also purchase advanced features to better manage your accounts.

Azure AD also offers other functionality, like managing integrated apps, that you can use to extend and customize your Microsoft 365 subscriptions.

You can use the Azure AD deployment advisors for a guided setup and configuration experience in the Microsoft 365 admin center (you must be signed in to Microsoft 365):

- [Azure AD Connect advisor](#)
- [AD FS deployment advisor](#)
- [Azure AD setup guide](#)

Azure AD editions and Microsoft 365 identity management

If you have a paid subscription to Microsoft 365, you also have a free Azure AD subscription. You can use Azure AD to create and manage user and group accounts. To activate this subscription, you have to complete a one-time registration. Afterward, you can access Azure AD from your Microsoft 365 admin center.

For instructions to register your free Azure AD subscription, see [use your free Azure AD subscription](#). Don't go directly to [azure.microsoft.com](#) to sign up or you'll end up with a trial or paid subscription to Microsoft Azure that is separate from your free Azure AD subscription with Microsoft 365.

With the free subscription you can synchronize with on-premises directories, set up single sign-on, and synchronize with many software as service applications, such as Salesforce, DropBox, and many more.

If you want enhanced AD DS functionality, bi-directional synchronization, and other management capabilities, you can upgrade your free subscription to a paid premium subscription. For the details, see [Azure Active Directory editions](#).

For more information about Microsoft 365 and Azure AD, see [Microsoft 365 identity models](#).

Extend the capabilities of your Microsoft 365 tenant

FEATURE	DESCRIPTION
Integrated apps	You can grant individual apps access to your Microsoft 365 data, such as mail, calendars, contacts, users, groups, files, and folders. You can also authorize these apps at Azure AD DC admin , or Global admin level and make them available to your entire company by registering the apps in Azure AD. For more information, see Integrated Apps and Azure AD for Microsoft 365 administrators . For more information, see About admin roles . Also see Single sign-on .

FEATURE	DESCRIPTION
Power Apps	Power Apps are focused apps for mobile devices that can connect to your existing data sources like SharePoint lists and other data apps. See Create a Power App for a list in SharePoint Online and the Power Apps page for details.

See also

[Microsoft 365 Enterprise overview](#)

Azure ExpressRoute for Office 365

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Learn how Azure ExpressRoute is used with Office 365 and how to plan the network implementation project that will be required if you're deploying Azure ExpressRoute for use with Office 365. Infrastructure and platform services running in Azure will often benefit by addressing network architecture and performance considerations. We recommend ExpressRoute for Azure in these cases. Software as a Service offerings like Office 365 and Dynamics 365 have been built to be accessed securely and reliably via the Internet. You can read about Internet performance and security and when you might consider Azure ExpressRoute for Office 365 in the article [Assessing Office 365 network connectivity](#).

NOTE

Microsoft Defender for Endpoint does not provide integration with Azure ExpressRoute. While this does not stop customers from defining ExpressRoute rules that enable connectivity from a private network to Microsoft Defender for Endpoint cloud services, it is up to the customer to maintain rules as the service or cloud infrastructure evolves.

NOTE

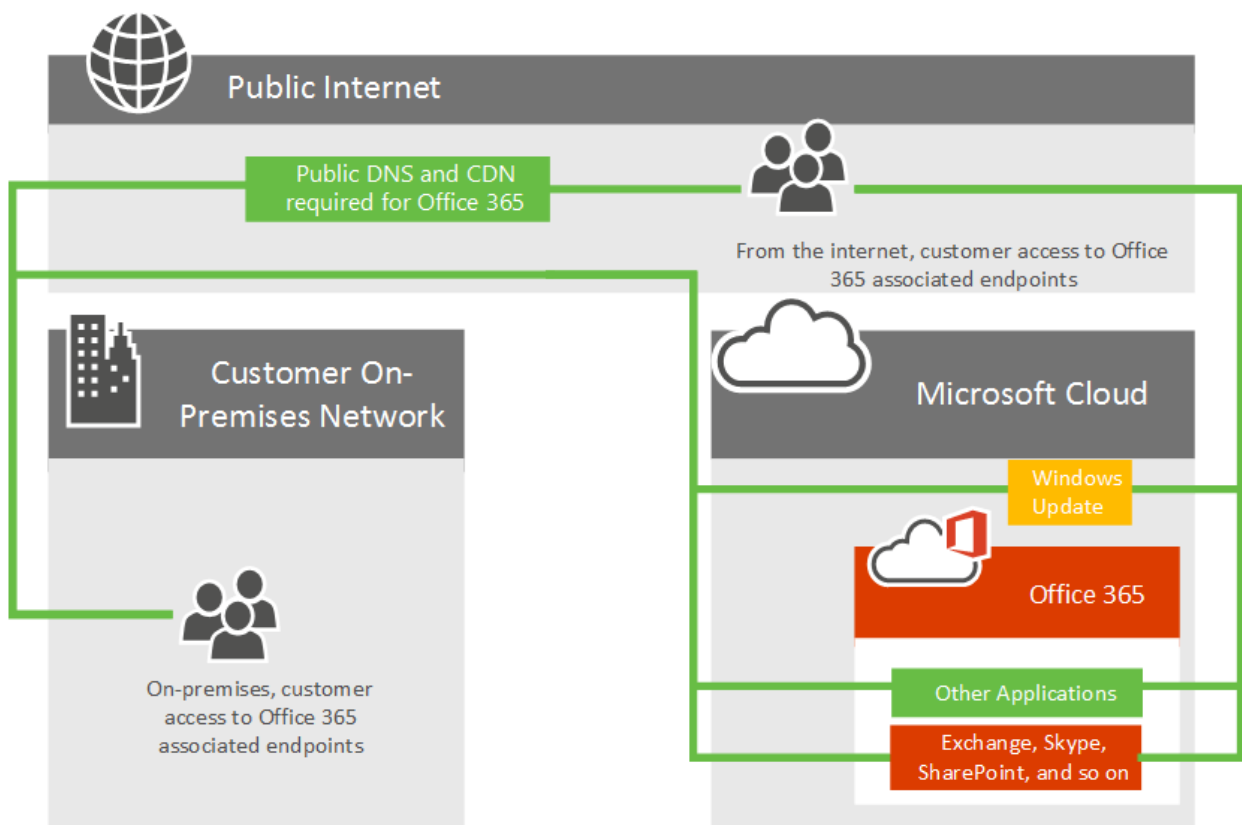
We do not recommend ExpressRoute for Microsoft 365 because it does not provide the best connectivity model for the service in most circumstances. As such, Microsoft authorization is required to use this connectivity model for Microsoft 365. We review every customer request and authorize ExpressRoute for Microsoft 365 only in the rare scenarios where it is necessary. Please read the [ExpressRoute for Microsoft 365 guide](#) for more information and following a comprehensive review of the document with your productivity, network, and security teams, work with your Microsoft account team to submit an exception if needed. Unauthorized subscriptions trying to create route filters for Office 365 will receive an [error message](#).

Planning Azure ExpressRoute for Office 365

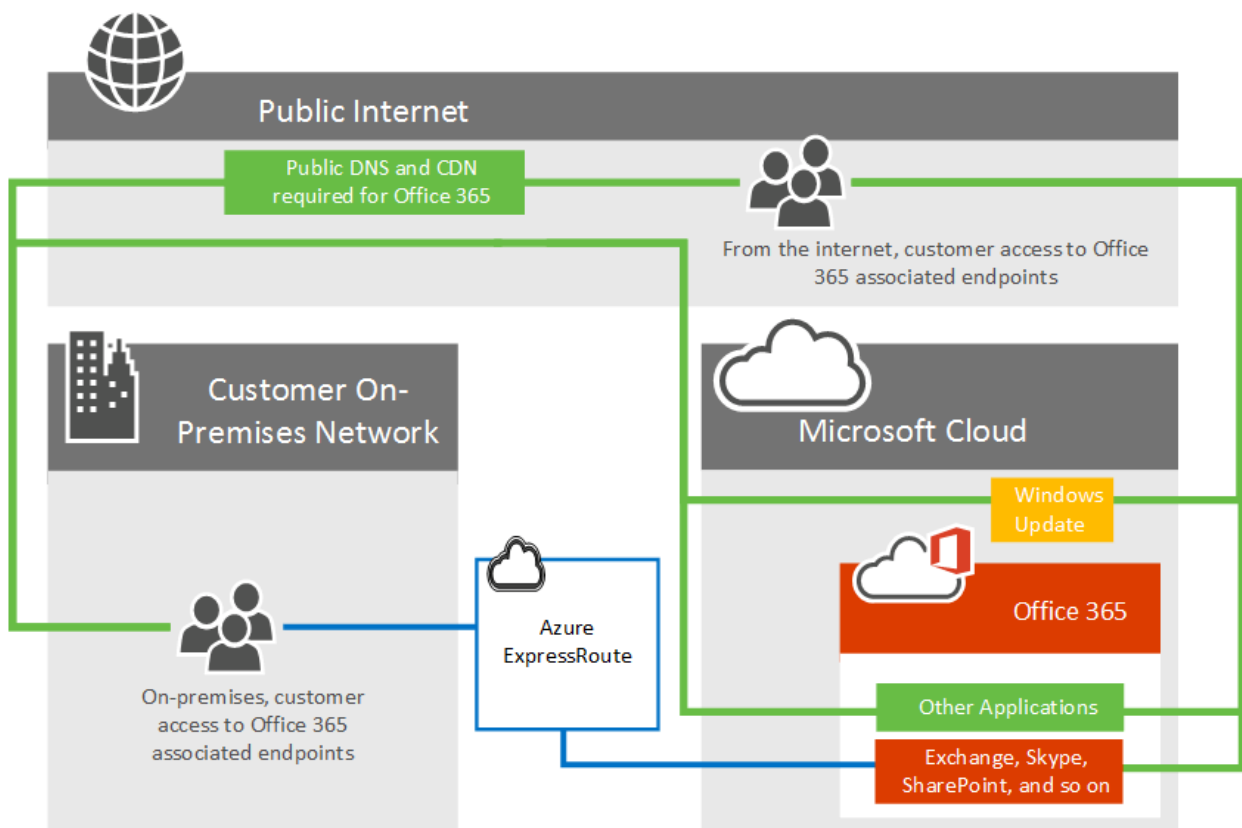
In addition to internet connectivity, you may choose to route a subset of their Office 365 network traffic over a direct connection that offers predictability and a 99.95% uptime SLA for the Microsoft networking components. Azure ExpressRoute provides you with this dedicated network connection to Office 365 and other Microsoft cloud services.

Regardless of whether you have an existing MPLS WAN, ExpressRoute can be added to your network architecture in one of three ways; through a supported cloud exchange co-location provider, an Ethernet point-to-point connection provider, or through an MPLS connection provider. See what [providers are available in your region](#). The direct ExpressRoute connection will enable connectivity to the applications outlined in [What Office 365 services are included?](#) below. Network traffic for all other applications and services will continue to traverse the internet.

Consider the following high level network diagram, which shows a typical Office 365 customer connecting to Microsoft's datacenters over the internet for access to all Microsoft applications such as Office 365, Windows Update, and TechNet. Customers use a similar network path regardless of whether they're connecting from an on-premises network or from an independent internet connection.



Now look at the updated diagram, which depicts an Office 365 customer who uses both the internet and ExpressRoute to connect to Office 365. Notice that some connections such as Public DNS and Content Delivery Network nodes still require the public internet connection. Also notice the customer's users who aren't located in their ExpressRoute connected building are connecting over the Internet.



Still want more information? Learn how to [manage your network traffic with Azure ExpressRoute for Office 365](#) and learn how to [configure Azure ExpressRoute for Office 365](#). We've also recorded a 10 part [Azure ExpressRoute for Office 365 Training](#) series on Channel 9 to help explain the concepts more thoroughly.

What Office 365 services are included?

The following table lists the Office 365 services that are supported over ExpressRoute. Review the [Office 365 endpoints article](#) to understand which network requests for these applications require internet connectivity.

APPLICATIONS INCLUDED
Exchange Online ¹ Exchange Online Protection ¹ Delve ¹
Skype for Business Online ¹ Microsoft Teams ¹
SharePoint Online ¹ OneDrive for Business ¹ Project Online ¹
Portal and shared ¹ Azure Active Directory (Azure AD) ¹ Azure AD Connect ¹ Office ¹

¹ Each of these applications has internet connectivity requirements not supported over ExpressRoute, see the [Office 365 endpoints article](#) for more information.

The services that aren't included with ExpressRoute for Office 365 are Microsoft 365 Apps for enterprise client downloads, On-premises Identity Provider Sign-In, and Office 365 (operated by 21 Vianet) service in China.

Implementing ExpressRoute for Office 365

Implementing ExpressRoute requires the involvement of network and application owners and requires careful planning to determine the new [network routing architecture](#), bandwidth requirements, where security will be implemented, high availability, and so on. To implement ExpressRoute, you'll need to:

1. Fully understand the need ExpressRoute satisfies in your Office 365 connectivity planning. Understand what applications will use the internet or ExpressRoute and fully plan your network capacity, security, and high availability needs in the context of using both the internet and ExpressRoute for Office 365 traffic.
2. Determine the egress and peering locations for both internet and ExpressRoute traffic¹.
3. Determine the capacity required on the internet and ExpressRoute connections.
4. Have a plan in place for implementing security and other standard perimeter controls¹.
5. Have a valid Microsoft Azure account to subscribe to ExpressRoute.
6. Select a connectivity model and an [approved provider](#). Keep in mind, customers can select multiple connectivity models or partners and the partner doesn't need to be the same as your existing network provider.
7. Validate deployment prior to directing traffic to ExpressRoute.
8. Optionally [implement QoS](#) and evaluate regional expansion.

¹ Important performance considerations. Decisions here can dramatically impact latency, which is a critical for applications such as Skype for Business.

For additional references, use our [routing guide](#) in addition to the [ExpressRoute documentation](#).

To purchase ExpressRoute for Office 365, you'll need to work with one or more [approved providers](#) to provision the desired number and size circuits with an ExpressRoute Premium subscription. There are no additional licenses to purchase from Office 365.

Here's a short link you can use to come back: <https://aka.ms/expressrouteoffice365>

Ready to sign up for [ExpressRoute for Office 365](#)?

Related Topics

[Assessing Office 365 network connectivity](#)

[Managing ExpressRoute for Office 365 connectivity](#)

[Routing with ExpressRoute for Office 365](#)

[Network planning with ExpressRoute for Office 365](#)

[Implementing ExpressRoute for Office 365](#)

[Using BGP communities in ExpressRoute for Office 365 scenarios](#)

[Media Quality and Network Connectivity Performance in Skype for Business Online](#)

[Office 365 performance tuning using baselines and performance history](#)

[Performance troubleshooting plan for Office 365](#)

[Office 365 URLs and IP address ranges](#)

[Office 365 network and performance tuning](#)

See also

[Microsoft 365 Enterprise overview](#)

Hybrid modern authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange servers

10/28/2022 • 10 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Modern Authentication is a method of identity management that offers more secure user authentication and authorization. It's available for Office 365 hybrid deployments of Skype for Business server on-premises and Exchange server on-premises, and split-domain Skype for Business hybrids. This article links to related docs about prerequisites, setup/disabling modern authentication, and to some of the related client (ex. Outlook and Skype clients) information.

- [What is modern authentication?](#)
- [What changes when I use modern authentication?](#)
- [Check the modern authentication status of your on-premises environment](#)
- [Do you meet modern authentication prerequisites?](#)
- [What else do I need to know before I begin?](#)

What is modern authentication?

Modern authentication is an umbrella term for a combination of authentication and authorization methods between a client (for example, your laptop or your phone) and a server, as well as some security measures that rely on access policies that you may already be familiar with. It includes:

- **Authentication methods:** Multifactor authentication (MFA); smart card authentication; client certificate-based authentication
- **Authorization methods:** Microsoft's implementation of Open Authorization (OAuth)
- **Conditional access policies:** Mobile Application Management (MAM) and Azure Active Directory (Azure AD) Conditional Access

Managing user identities with modern authentication gives administrators many different tools to use when it comes to securing resources and offers more secure methods of identity management to both on-premises (Exchange and Skype for Business), Exchange hybrid, and Skype for Business hybrid/split-domain scenarios.

Because Skype for Business works closely with Exchange, the login behavior Skype for Business client users will be affected by the modern authentication status of Exchange. It is also applicable if you have a Skype for Business *split-domain* hybrid architecture, in which you have both Skype for Business Online and Skype for Business on-premises, with users homed in both locations.

For more information about modern authentication in Office 365, see [Office 365 Client App Support - Multifactor authentication](#).

IMPORTANT

As of August of 2017, all new Office 365 tenants that include Skype for Business online and Exchange online will have modern authentication enabled by default. Pre-existing tenants won't have a change in their default MA state, but all new tenants automatically support the expanded set of identity features you see listed above. To check your MA status, see the [Check the modern authentication status of your on-premises environment](#) section.

What changes when I use modern authentication?

When using modern authentication with on-premises Skype for Business or Exchange server, you're still *authenticating* users on-premises, but the story of *authorizing* their access to resources (like files or emails) changes. This is why, though modern authentication is about client and server communication, the steps taken during configuring MA result in evoSTS (a Security Token Service used by Azure AD) being set as Auth Server for Skype for Business and Exchange server on-premises.

The change to evoSTS allows your on-premises servers to take advantage of OAuth (token issuance) for authorizing your clients, and also lets your on-premises use security methods common in the cloud (like Multi-factor Authentication). Additionally, the evoSTS issues tokens that allow users to request access to resources without supplying their password as part of the request. No matter where your users are homed (of online or on-premises), and no matter which location hosts the needed resource, EvoSTS will become the core of authorizing users and clients once modern authentication is configured.

For example, if a Skype for Business client needs to access Exchange server to get calendar information on behalf of a user, it uses the Microsoft Authentication Library (MSAL) to do so. MSAL is a code library designed to make secured resources in your directory available to client applications using OAuth security tokens. MSAL works with OAuth to verify claims and to exchange tokens (rather than passwords), to grant a user access to a resource. In the past, the authority in a transaction like this one--the server that knows how to validate user claims and issue the needed tokens--might have been a Security Token Service on-premises, or even Active Directory Federation Services. However, modern authentication centralizes that authority by using Azure AD.

This also means that even though your Exchange server and Skype for Business environments may be entirely on-premises, the authorizing server will be online, and your on-premises environment must have the ability to create and maintain a connection to your Office 365 subscription in the Cloud (and the Azure AD instance that your subscription uses as its directory).

What doesn't change? Whether you're in a split-domain hybrid or using Skype for Business and Exchange server on-premises, all users must first authenticate *on-premises*. In a hybrid implementation of modern authentication, *Lyncdiscovery* and *Autodiscovery* both point to your on-premises server.

IMPORTANT

If you need to know the specific Skype for Business topologies supported with MA, that's [documented right here](#).

Check the modern authentication status of your on-premises environment

Because modern authentication changes the authorization server used when services apply OAuth/S2S, you need to know if modern authentication is enabled or disabled for your on-premises Skype for Business and Exchange environments. You can check the status on your Exchange servers by running the following PowerShell command:

If the value of the *OAuth2ClientProfileEnabled* property is **False**, then modern authentication is disabled.

For more information about the Get-OrganizationConfig cmdlet, see [Get-OrganizationConfig](#).

You can check your Skype for Business servers by running the following PowerShell command:

```
Get-CsOAuthConfiguration
```

If the command returns an empty *OAuthServers* property, or if the value of the *ClientADALAuthOverride* property is not **Allowed**, then modern authentication is disabled.

For more information about the Get-CsOAuthConfiguration cmdlet, see [Get-CsOAuthConfiguration](#).

Do you meet modern authentication prerequisites?

Verify and check these items off your list before you continue:

- **Skype for Business specific**
 - All servers must have May 2017 cumulative update (CU5) for Skype for Business Server 2015 or later
 - **Exception** - Survivability Branch Appliance (SBA) can be on the current version (based on Lync 2013)
 - Your SIP domain is added as a Federated domain in Office 365
 - All SFB Front Ends must have connections outbound to the internet, to Office 365 Authentication URLs (TCP 443) and well-known certificate root CRLs (TCP 80) listed in Rows 56 and 125 of the 'Microsoft 365 Common and Office' section of [Office 365 URLs and IP address ranges](#).
- **Skype for Business on-premises in a hybrid Office 365 environment**
 - A Skype for Business Server 2019 deployment with all servers running Skype for Business Server 2019.
 - A Skype for Business Server 2015 deployment with all servers running Skype for Business Server 2015.
 - A deployment with a maximum of two different server versions as listed below:
 - Skype for Business Server 2015
 - Skype for Business Server 2019
 - All Skype for Business servers must have the latest cumulative updates installed, see [Skype for Business Server updates](#) to find and manage all available updates.
 - There is no Lync Server 2010 or 2013 in the hybrid environment.

NOTE

If your Skype for Business front-end servers use a proxy server for Internet access, the proxy server IP and Port number used must be entered in the configuration section of the web.config file for each front end.

- C:\Program Files\Skype for Business Server 2015\Web Components\Web ticket\int\web.config
- C:\Program Files\Skype for Business Server 2015\Web Components\Web ticket\ext\web.config

```
<configuration>
  <system.net>
    <defaultProxy>
      <proxy
        proxyaddress="https://192.168.100.60:8080"
        bypassonlocal="true" />
    </defaultProxy>
  </system.net>
</configuration>
```

IMPORTANT

Be sure to subscribe to the RSS feed for [Office 365 URLs and IP address ranges](#) to stay current with the latest listings of required URLs.

- **Exchange Server specific**

- You're using either Exchange server 2013 CU19 and up, Exchange server 2016 CU8 and up, or Exchange Server 2019 CU1 and up.
- There is no Exchange server 2010 in the environment.
- SSL Offloading is not configured. SSL termination and re-encryption are supported.
- In the event your environment utilizes a proxy server infrastructure to allow servers to connect to the Internet, be sure all Exchange servers have the proxy server defined in the [InternetWebProxy](#) property.

- **Exchange Server on-premises in a hybrid Office 365 environment**

- If you are using Exchange Server 2013, at least one server must have the Mailbox and Client Access server roles installed. While it is possible to install the Mailbox and Client Access roles on separate servers, we strongly recommend that you install both roles on the same server to provide more reliability and improved performance.
- If you are using Exchange server 2016 or later version, at least one server must have the Mailbox server role installed.
- There is no Exchange server 2007 or 2010 in the Hybrid environment.
- All Exchange servers must have the latest cumulative updates installed, see [Upgrade Exchange to the latest Cumulative Updates](#) to find and manage all available updates.

- **Exchange client and protocol requirements**

The availability of modern authentication is determined by the combination of the client, protocol, and configuration. If modern authentication is not supported by the client, protocol, and/or configuration, then the client will continue to use legacy authentication.

The following clients and protocols support modern authentication with on-premises Exchange when modern authentication is enabled in the environment:

CLIENTS	PRIMARY PROTOCOL	NOTES
---------	------------------	-------

CLIENTS	PRIMARY PROTOCOL	NOTES
Outlook 2013 and later	MAPI over HTTP	MAPI over HTTP must be enabled within Exchange in order to use modern authentication with these clients (enabled or True for new installs of Exchange 2013 Service Pack 1 and above); for more information, see How modern authentication works for Office 2013 and Office 2016 client apps . Ensure you are running the minimum required build of Outlook; see Latest updates for versions of Outlook that use Windows Installer (MSI) .
Outlook 2016 for Mac and later	Exchange Web Services	
Outlook for iOS and Android	Microsoft sync technology	See Using hybrid Modern Authentication with Outlook for iOS and Android for more information.
Exchange ActiveSync clients (for example, iOS11 Mail)	Exchange ActiveSync	For Exchange ActiveSync clients that support modern authentication, you must recreate the profile in order to switch from basic authentication to modern authentication.

Clients and/or protocols that are not listed (for example, POP3) do not support modern authentication with on-premises Exchange and continue to use legacy authentication mechanisms even after modern authentication is enabled in the environment.

• General prerequisites

- Resource forest scenarios will require a two-way trust with the account forest to ensure proper SID lookups are performed during hybrid modern authentication requests.
- If you use AD FS, you should have Windows 2012 R2 AD FS 3.0 and above for federation.
- Your identity configurations are any of the types supported by Azure AD Connect, such as password hash sync, pass-through authentication, and on-premises STS supported by Office 365.
- You have Azure AD Connect configured and functioning for user replication and sync.
- You have verified that hybrid is configured using Exchange Classic Hybrid Topology mode between your on-premises and Office 365 environment. Official support statement for Exchange hybrid says you must have either current CU or current CU - 1.

NOTE

Hybrid modern authentication is not supported with the [Hybrid Agent](#).

- Make sure both an on-premises test user, as well as a hybrid test user homed in Office 365, can login to the Skype for Business desktop client (if you want to use modern authentication with Skype) and Microsoft Outlook (if you want to use modern authentication with Exchange).
- Make sure the SignInOptions setting in Microsoft Office is not configured to its most restrictive setting. For more information, see [How to allow Office to connect to the internet](#).

What else do I need to know before I begin?

- All the scenarios for on-premises servers involve setting up modern authentication on-premises (in fact, for Skype for Business there is a list of supported topologies) so that the server responsible for authentication and authorization is in the Microsoft Cloud (Azure AD's security token service, called 'evoSTS'), and updating Azure AD about the URLs or namespaces used by your on-premises installation of either Skype for Business or Exchange. Therefore, on-premises servers take on a Microsoft Cloud dependency. Taking this action could be considered configuring 'hybrid auth'.
- This article links out to others that will help you choose supported modern authentication topologies (necessary only for Skype for Business), and how-to articles that outline the setup steps, or steps to disable modern authentication, for Exchange on-premises and Skype for Business on-premises. Favorite this page in your browser if you're going to need a home-base for using modern authentication in your server environment.

Related Topics

- [How to configure Exchange Server on-premises to use Modern Authentication](#)
- [Skype for Business topologies supported with Modern Authentication](#)
- [How to configure Skype for Business on-premises to use Modern Authentication](#)
- [Removing or disabling Hybrid Modern Authentication from Skype for Business and Exchange](#)

How to configure Exchange Server on-premises to use Hybrid Modern Authentication

10/28/2022 • 6 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Hybrid Modern Authentication (HMA) is a method of identity management that offers more secure user authentication and authorization, and is available for Exchange server on-premises hybrid deployments.

Definitions

Before we begin, you should be familiar with some definitions:

- Hybrid Modern Authentication > HMA
- Exchange on-premises > EXCH
- Exchange Online > EXO

Also, if a graphic in this article has an object that's 'grayed-out' or 'dimmed' that means the element shown in gray is not included in HMA-specific configuration.

Enabling Hybrid Modern Authentication

Turning on HMA means:

1. Being sure you meet the prereqs before you begin.
2. Since many **prerequisites** are common for both Skype for Business and Exchange, [Hybrid Modern Authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange servers](#). Do this before you begin any of the steps in this article. Requirements about linked mailboxes to be inserted.
3. Adding on-premises web service URLs as **Service Principal Names (SPNs)** in Azure AD. In case EXCH is in hybrid with **multiple tenants**, these on-premises web service URLs must be added as SPNs in the Azure AD of all the tenants which are in hybrid with EXCH.
4. Ensuring all Virtual Directories are enabled for HMA
5. Checking for the EvoSTS Auth Server object
6. Enabling HMA in EXCH.

NOTE

Does your version of Office support MA? See [How modern authentication works for Office 2013 and Office 2016 client apps](#).

Make sure you meet all the prerequisites

Since many prerequisites are common for both Skype for Business and Exchange, review [Hybrid Modern Authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange](#)

[servers](#). Do this *before* you begin any of the steps in this article.

NOTE

Outlook Web App and Exchange Control Panel do not work with hybrid Modern Authentication. In addition, publishing Outlook Web App and Exchange Control Panel through Azure AD Application Proxy is unsupported.

Add on-premises web service URLs as SPNs in Azure AD

Run the commands that assign your on-premises web service URLs as Azure AD SPNs. SPNs are used by client machines and devices during authentication and authorization. All the URLs that might be used to connect from on-premises to Azure Active Directory (Azure AD) must be registered in Azure AD (this includes both internal and external namespaces).

First, gather all the URLs that you need to add in AAD. Run these commands on-premises:

```
Get-MapiVirtualDirectory | FL server,*url*
Get-WebServicesVirtualDirectory | FL server,*url*
Get-ClientAccessServer | fl Name, AutodiscoverServiceInternalUri
Get-OABVirtualDirectory | FL server,*url*
Get-AutodiscoverVirtualDirectory | FL server,*url*
Get-OutlookAnywhere | FL server,*hostname*
```

Ensure the URLs clients may connect to are listed as HTTPS service principal names in AAD. In case EXCH is in hybrid with **multiple tenants**, these HTTPS SPNs should be added in the AAD of all the tenants in hybrid with EXCH.

1. First, connect to AAD with [these instructions](#).

NOTE

You need to use the *Connect-MsolService* option from this page to be able to use the command below.

2. For your Exchange-related URLs, type the following command:

```
Get-MsolServicePrincipal -AppPrincipalId 00000002-0000-0ff1-ce00-000000000000 | select -
ExpandProperty ServicePrincipalNames
```

Take note of (and screenshot for later comparison) the output of this command, which should include an `https://*autodiscover.yourdomain.com*` and `https://*mail.yourdomain.com*` URL, but mostly consist of SPNs that begin with `00000002-0000-0ff1-ce00-000000000000/`. If there are `https://` URLs from your on-premises that are missing, those specific records should be added to this list.

3. If you don't see your internal and external MAPI/HTTP, EWS, ActiveSync, OAB, and Autodiscover records in this list, you must add them using the command below (the example URLs are `mail.corp.contoso.com` and `owa.contoso.com`, but you'd **replace the example URLs with your own**):

```
$x= Get-MsolServicePrincipal -AppPrincipalId 00000002-0000-0ff1-ce00-000000000000
$x.ServicePrincipalNames.Add("https://mail.corp.contoso.com/")
$x.ServicePrincipalNames.Add("https://owa.contoso.com/")
Set-MSOLServicePrincipal -AppPrincipalId 00000002-0000-0ff1-ce00-000000000000 -ServicePrincipalNames
$x.ServicePrincipalNames
```

4. Verify your new records were added by running the `Get-MsolServicePrincipal` command from step 2

again, and looking through the output. Compare the list / screenshot from before to the new list of SPNs. You might also take a screenshot of the new list for your records. If you were successful, you will see the two new URLs in the list. Going by our example, the list of SPNs will now include the specific URLs

```
https://mail.corp.contoso.com and https://owa.contoso.com .
```

Verify Virtual Directories are Properly Configured

Now verify OAuth is properly enabled in Exchange on all of the Virtual Directories Outlook might use by running the following commands:

```
Get-MapiVirtualDirectory | FL server,*url*,*auth*
Get-WebServicesVirtualDirectory | FL server,*url*,*oauth*
Get-OABVirtualDirectory | FL server,*url*,*oauth*
Get-AutoDiscoverVirtualDirectory | FL server,*oauth*
```

Check the output to make sure **OAuth** is enabled on each of these VDirs, it will look something like this (and the key thing to look at is 'OAuth'):

```
Get-MapiVirtualDirectory | fl server,*url*,*auth*

Server                : EX1
InternalUrl           : https://mail.contoso.com/mapi
ExternalUrl           : https://mail.contoso.com/mapi
IISAuthenticationMethods : {Ntlm, OAuth, Negotiate}
InternalAuthenticationMethods : {Ntlm, OAuth, Negotiate}
ExternalAuthenticationMethods : {Ntlm, OAuth, Negotiate}
```

If OAuth is missing from any server and any of the four virtual directories, you need to add it by using the relevant commands before proceeding ([Set-MapiVirtualDirectory](#), [Set-WebServicesVirtualDirectory](#), [Set-OABVirtualDirectory](#), and [Set-AutodiscoverVirtualDirectory](#)).

Confirm the EvoSTS Auth Server Object is Present

Return to the on-premises Exchange Management Shell for this last command. Now you can validate that your on-premises has an entry for the evoSTS authentication provider:

```
Get-AuthServer | where {$_.Name -like "EvoSts*"} | ft name,enabled
```

Your output should show an AuthServer of the Name EvoSts with a GUID and the 'Enabled' state should be True. If you don't see this, you should download and run the most recent version of the Hybrid Configuration Wizard.

NOTE

In case EXCH is in hybrid with **multiple tenants**, your output should show one AuthServer of the Name

```
EvoSts - {GUID}
```

for each tenant in hybrid with EXCH and the **Enabled** state should be True for all of these AuthServer objects.

IMPORTANT

If you're running Exchange 2010 in your environment, the EvoSTS authentication provider won't be created.

Enable HMA

Run the following command in the Exchange Management Shell, on-premises, replacing <GUID> in the command line with the string in your environment:

```
Set-AuthServer -Identity "EvoSTS - <GUID>" -IsDefaultAuthorizationEndpoint $true
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

NOTE

In older versions of the Hybrid Configuration Wizard the EvoSTS AuthServer was simply named EvoSTS without a GUID attached. There is no action you need to take, just modify the command line above to reflect this by removing the GUID portion of the command:

```
Set-AuthServer -Identity EvoSTS -IsDefaultAuthorizationEndpoint $true
```

If the EXCH version is Exchange 2016 (CU18 or higher) or Exchange 2019 (CU7 or higher) and hybrid was configured with HCW downloaded after September 2020, run the following command in the Exchange Management Shell, on-premises:

```
Set-AuthServer -Identity "EvoSTS - {GUID}" -DomainName "Tenant Domain" -IsDefaultAuthorizationEndpoint $true
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

NOTE

In case EXCH is in hybrid with **multiple tenants**, there are multiple AuthServer objects present in EXCH with domains corresponding to each tenant. The **IsDefaultAuthorizationEndpoint** flag should be set to true (using the **IsDefaultAuthorizationEndpoint** cmdlet) for any one of these AuthServer objects. This flag can't be set to true for all the Authserver objects and HMA would be enabled even if one of these AuthServer object's **IsDefaultAuthorizationEndpoint** flag is set to true.

For the **DomainName** parameter, use the tenant domain value, which is usually in the form `contoso.onmicrosoft.com`.

Verify

Once you enable HMA, a client's next login will use the new auth flow. Note that just turning on HMA won't trigger a reauthentication for any client, and it might take a while for Exchange to pick up the new settings.

You should also hold down the CTRL key at the same time you right-click the icon for the Outlook client (also in the Windows Notifications tray) and click 'Connection Status'. Look for the client's SMTP address against an **Authn** type of `Bearer\*`, which represents the bearer token used in OAuth.

NOTE

Need to configure Skype for Business with HMA? You'll need two articles: One that lists [supported topologies](#), and one that shows you [how to do the configuration](#).

Using hybrid Modern Authentication with Outlook for iOS and Android

If you are an on-premises customer using Exchange server on TCP 443, allow network traffic from the following IP ranges:

52.125.128.0/20
52.127.96.0/23

These IP address ranges are also documented in [Additional endpoints not included in the Office 365 IP Address and URL Web service](#).

Related topics

[Modern Authentication configuration requirements for transition from Office 365 dedicated/ITAR to vNext](#)

How to configure Skype for Business on-premises to use Hybrid Modern Authentication

10/28/2022 • 6 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Modern Authentication, is a method of identity management that offers more secure user authentication and authorization, is available for Skype for Business server on-premises and Exchange server on-premises, and split-domain Skype for Business hybrids.

IMPORTANT

Would you like to know more about Modern Authentication (MA) and why you might prefer to use it in your company or organization? Check [this document](#) for an overview. If you need to know what Skype for Business topologies are supported with MA, that's documented [here](#)!

Before we begin, I use these terms:

- Modern Authentication (MA)
- Hybrid Modern Authentication (HMA)
- Exchange on-premises (EXCH)
- Exchange Online (EXO)
- Skype for Business on-premises (SFB)
- Skype for Business Online (SFBO)

Also, if a graphic in this article has an object that's grayed-out or dimmed that means the element shown in gray isn't included in MA-specific configuration.

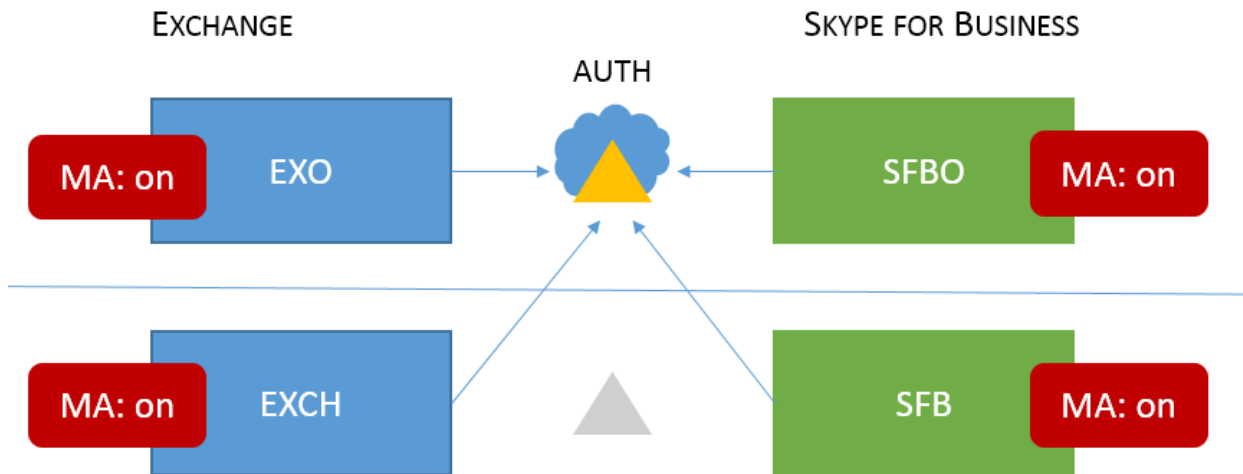
Read the summary

This summary breaks down the process into steps that might otherwise get lost during the execution, and is good for an overall checklist to keep track of where you are in the process.

1. First, make sure you meet all the prerequisites.
2. Since many **prerequisites** are common for both Skype for Business and Exchange, [see the overview article for your pre-req checklist](#). Do this *before* you begin any of the steps in this article.
3. Collect the HMA-specific info you'll need in a file, or OneNote.
4. Turn ON Modern Authentication for EXO (if it isn't already turned on).
5. Turn ON Modern Authentication for SFBO (if it isn't already turned on).
6. Turn ON Hybrid Modern Authentication for Exchange on-premises.
7. Turn ON Hybrid Modern Authentication for Skype for Business on-premises.

These steps turn on MA for SFB, SFBO, EXCH, and EXO - that is, all the products that can participate in an HMA configuration of SFB and SFBO (including dependencies on EXCH/EXO). In other words, if your users are homed

in/have mailboxes created in any part of the Hybrid (EXO + SFBO, EXO + SFB, EXCH + SFBO, or EXCH + SFB), your finished product will look like this:



As you can see there are four different places to turn on MA! For the best user experience, we recommend you turn on MA in all four of these locations. If you can't turn MA on in all these locations, adjust the steps so that you turn on MA only in the locations that are necessary for your environment.

See the [Supportability](#) topic for [Skype for Business with MA](#) for supported topologies.

IMPORTANT

Double-check that you've met all the prerequisites before you begin. You'll find that information in [Hybrid modern authentication overview and prerequisites](#).

Collect all HMA-specific info you'll need

After you've double-checked that you meet the [prerequisites](#) to use Modern Authentication (see the note above), you should create a file to hold the info you'll need for configuring HMA in the steps ahead. Examples used in this article:

- **SIP/SMTP domain**
 - Ex. contoso.com (is federated with Office 365)
- **Tenant ID**
 - The GUID that represents your Office 365 tenant (at the login of contoso.onmicrosoft.com).
- **SFB 2015 CU5 Web Service URLs**

You'll need internal and external web service URLs for all Sfb 2015 pools deployed. To obtain these, run the following from Skype for Business Management Shell:

```
Get-CsService -WebServer | Select-Object PoolFqdn, InternalFqdn, ExternalFqdn | FL
```

- Ex. Internal: <https://lyncwebint01.contoso.com>
- Ex. External: <https://lyncwebext01.contoso.com>

If you're using a Standard Edition server, the internal URL will be blank. In this case, use the pool fqdn for the internal URL.

Turn on Modern Authentication for EXO

Follow the instructions here: [Exchange Online: How to enable your tenant for modern authentication](#).

Turn on Modern Authentication for SFBO

Follow the instructions here: [Skype for Business Online: Enable your tenant for modern authentication](#).

Turn on Hybrid Modern Authentication for Exchange on-premises

Follow the instructions here: [How to configure Exchange Server on-premises to use Hybrid Modern Authentication](#).

Turn on Hybrid Modern Authentication for Skype for Business on-premises

Add on-premises web service URLs as SPNs in Azure Active Directory

Now you'll need to run commands to add the URLs (collected earlier) as Service Principals in SFBO.

NOTE

Service principal names (SPNs) identify web services and associate them with a security principal (such as an account name or group) so that the service can act on the behalf of an authorized user. Clients authenticating to a server make use of information that's contained in SPNs.

1. First, connect to Azure Active Directory (Azure AD) with [these instructions](#).
2. Run this command, on-premises, to get a list of SFB web service URLs.

Note that the AppPrincipalId begins with `00000004`. This corresponds to Skype for Business Online.

Take note of (and screenshot for later comparison) the output of this command, which will include an SE and WS URL, but mostly consist of SPNs that begin with `00000004-0000-0ff1-ce00-000000000000/`.

```
Get-MsolServicePrincipal -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000 | Select -  
ExpandProperty ServicePrincipalNames
```

3. If the internal **or** external SFB URLs from on-premises are missing (for example, <https://lyncwebint01.contoso.com> and <https://lyncwebext01.contoso.com>) we will need to add those specific records to this list.

Be sure to replace *the example URLs* below with your actual URLs in the Add commands!

```
$x= Get-MsolServicePrincipal -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000  
$x.ServicePrincipalNames.Add("https://lyncwebint01.contoso.com/")  
$x.ServicePrincipalNames.Add("https://lyncwebext01.contoso.com/")  
Set-MSOLServicePrincipal -AppPrincipalId 00000004-0000-0ff1-ce00-000000000000 -ServicePrincipalNames  
$x.ServicePrincipalNames
```

4. Verify your new records were added by running the **Get-MsolServicePrincipal** command from step 2 again, and looking through the output. Compare the list or screenshot from before to the new list of SPNs. You might also screenshot the new list for your records. If you were successful, you'll see the two new URLs in the list. Going by our example, the list of SPNs will now include the specific URLs <https://lyncwebint01.contoso.com> and <https://lyncwebext01.contoso.com/>.

Create the EvoSTS Auth Server Object

Run the following command in the Skype for Business Management Shell.

```
New-CsOAuthServer -Identity evoSTS -MetadataURL https://login.windows.net/common/FederationMetadata/2007-06/FederationMetadata.xml -AcceptSecurityIdentifierInformation $true -Type AzureAD
```

Enable Hybrid Modern Authentication

This is the step that actually turns on MA. All the previous steps can be run ahead of time without changing the client authentication flow. When you're ready to change the authentication flow, run this command in the Skype for Business Management Shell.

```
Set-CsOAuthConfiguration -ClientAuthorizationOAuthServerIdentity evoSTS
```

Verify

Once you enable HMA, a client's next login will use the new auth flow. Note that just turning on HMA won't trigger a reauthentication for any client. The clients reauthenticate based on the lifetime of the auth tokens and/or certs they have.

To test that HMA is working after you've enabled it, sign out of a test SFB Windows client and be sure to click 'delete my credentials'. Sign in again. The client should now use the Modern Auth flow and your login will now include an **Office 365** prompt for a 'Work or school' account, seen right before the client contacts the server and logs you in.

You should also check the 'Configuration Information' for Skype for Business Clients for an 'OAuth Authority'. To do this on your client computer, hold down the CTRL key at the same time you right-click the Skype for Business Icon in the Windows Notification tray. Click **Configuration Information** in the menu that appears. In the 'Skype for Business Configuration Information' window that will appear on the desktop, look for the following:

Lync OAUTH Authority URL	https://login.windows.net/common/oauth2/authorize
EWS OAUTH Authority URL	https://login.windows.net/common/oauth2/authorize

You should also hold down the CTRL key at the same time you right-click the icon for the Outlook client (also in the Windows Notifications tray) and click 'Connection Status'. Look for the client's SMTP address against an AuthN type of 'Bearer*', which represents the bearer token used in OAuth.

Related articles

[Link back to the Modern Authentication overview.](#)

Do you need to know how to use Modern Authentication for your Skype for Business clients? We've got steps here: [Hybrid modern authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange servers.](#)

Removing or disabling Hybrid Modern Authentication from Skype for Business and Exchange

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you've enabled Hybrid Modern Authentication (HMA) only to find it's unsuitable for your current environment, you can disable HMA. This article explains how.

Who is this article for?

If you've enabled Modern Authentication in Skype for Business Online or On-premises, and/or Exchange Online or On-premises and found you need to disable HMA, these steps are for you.

IMPORTANT

See the '[Skype for Business topologies supported with Modern Authentication](#)' article if you're in Skype for Business Online or On-premises, have a mixed-topology HMA, and need to look at supported topologies before you begin.

How to disable Hybrid Modern Authentication (Exchange)

1. **Exchange On-premises:** [Open the Exchange Management Shell](#) and run the following commands:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $false  
Set-AuthServer -Identity evoSTS -IsDefaultAuthorizationEndpoint $false
```

2. **Exchange Online:** [Connect to Exchange Online PowerShell](#). Run the following command to disable Modern Authentication:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled:$false
```

How to disable Hybrid Modern Authentication (Skype for Business)

1. **Skype for Business On-premises:** Run the following commands in Skype for Business Management Shell:

```
Set-CsOAuthConfiguration -ClientAuthorizationOAuthServerIdentity ""
```

2. **Skype for Business Online:** [Connect to Skype for Business Online PowerShell](#). Run the following command to disable Modern Authentication:

```
Set-CsOAuthConfiguration -ClientAdalAuthOverride Disallowed
```

[Link back to the Modern Authentication overview.](#)

How modern authentication works for Office 2013, Office 2016, and Office 2019 client apps

10/28/2022 • 9 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Read this article to learn how Office 2013, Office 2016, and Office 2019 client apps use modern authentication features based on the authentication configuration on the Microsoft 365 tenant for Exchange Online, SharePoint Online, and Skype for Business Online.

NOTE

Legacy client apps, such as Office 2010 and Office for Mac 2011, do not support modern authentication and can only be used with basic authentication.

Availability of modern authentication for Microsoft 365 services

For the Microsoft 365 services, the default state of modern authentication is:

- Turned **on** for Exchange Online by default. See [Enable or disable modern authentication in Exchange Online](#) to turn it off or on.
- Turned **on** for SharePoint Online by default.
- Turned **on** for Skype for Business Online by default. See [Enable Skype for Business Online for modern authentication](#) to turn it off or on.

NOTE

For tenants created **before** August 1, 2017, modern authentication is turned **off** by default for Exchange Online and Skype for Business Online.

Sign-in behavior of Office client apps

Office 2013 client apps support legacy authentication by default. Legacy means that they support either Microsoft Online Sign-in Assistant or basic authentication. In order for these clients to use modern authentication features, the Windows client must have registry keys set. For instructions, see [Enable Modern Authentication for Office 2013 on Windows devices](#).

IMPORTANT

The use of basic authentication is being deprecated for Exchange Online mailboxes on Microsoft 365. This means that if Outlook 2013 is not configured to use modern authentication, it loses the ability to connect. Read [this article](#) for more information about basic auth deprecation.

To enable modern authentication for any devices running Windows (for example on laptops and tablets), that have Microsoft Office 2013 installed, you need to set the following registry keys. The keys have to be set on each device that you want to enable for modern authentication:

REGISTRY KEY	TYPE	VALUE
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL	REG_DWORD	1
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version	REG_DWORD	1
HKEY_CURRENT_USER\Software\Microsoft\Exchange\AlwaysUseMSOAuthForAutoDiscover	REG_DWORD	1

Read [How to use Modern Authentication \(ADAL\) with Skype for Business](#) to learn about how it works with Skype for Business.

Software requirements

To enable multifactor authentication (MFA) for Office 2013 client apps, you must have the software listed below installed (at the version listed below, or a *later* version). The process is different depending on your installation type (either MSI-based, or via Click-to-run.)

First, find out if your Office installation is MSI-based or Click-to-run with the steps below.

1. Start Outlook 2013.
2. On the **File** menu, select **Office Account**.
3. For Outlook 2013 *Click-to-Run* installations an **Update Options** item is displayed. For MSI-based installations, the Update Options item is not displayed.
 - a. The Click-to-run **Update Options** button will tell you 'Updates are automatically downloaded and installed', and your current version.

Click-to-run based installations

For Click-to-run based installations you *must* have the following software installed at a file version listed below, or a *later* file version. If your file version is not equal to, or greater than, the file version listed, update it using the steps below.

FILE NAME	INSTALL PATH ON YOUR COMPUTER	FILE VERSION
MSO.DLL	C:\Program Files\Microsoft Office 15\root\vfs\ProgramFilesCommonx86\Microsoft Shared\OFFICE15\MSO.DLL	15.0.4753.1001
CSI.DLL	CSI.DLL C:\Program Files\Microsoft Office 15\root\office15\csi.dll	15.0.4753.1000
Groove.EXE*	C:\Program Files\Microsoft Office 15\root\office15\GROOVE.exe	15.0.4763.1000
Outlook.exe	C:\Program Files\Microsoft Office 15\root\office15\OUTLOOK.exe	15.0.4753.1002
ADAL.DLL	C:\Program Files\Microsoft Office 15\root\vfs\ProgramFilesCommonx86\Microsoft Shared\OFFICE15\ADAL.DLL	1.0.2016.624

FILE NAME	INSTALL PATH ON YOUR COMPUTER	FILE VERSION
lexplore.exe	C:\Program Files\Internet Explorer	varies

* If the Groove.EXE component is not present in your Office installation, it doesn't need to be installed for ADAL to work. However, if it is present, then the build for Groove.EXE listed here is required.

MSI-based installations

For MSI-based installations the following software *must* be installed at the file version listed below, or a *later* file version. If your file version is not equal to, or greater than, the file version listed below, update using the link in the *Update KB Article* column.

FILE NAME	INSTALL PATH ON YOUR COMPUTER	WHERE TO GET THE UPDATE	VERSION
MSO.DLL	C:\Program Files\Common Files\Microsoft Shared\OFFICE15\MSO.DLL	KB3085480	15.0.4753.1001
CSI.DLL	C:\Program Files\Common Files\Microsoft Shared\OFFICE15\Csi.dll	KB3172545	15.0.4753.1000
Groove.exe*	C:\Program Files\Microsoft Office\Office15\GROOVE.EXE	KB4022226	15.0.4763.1000
Outlook.exe	C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE	KB4484096	15.0.4753.1002
ADAL.DLL	C:\Program Files\Common Files\Microsoft Shared\OFFICE15\ADAL.DLL	KB3085565	1.0.2016.624
lexplore.exe	C:\Program Files\Internet Explorer	MS14-052	Not applicable

* If the Groove.EXE component is not present in your Office installation, it doesn't need to be installed for ADAL to work. However, if it is present, then the build for Groove.EXE listed here is required.

Office 2016 and Office 2019 clients support modern authentication by default, and no action is needed for the client to use these new flows. However, explicit action is needed to use legacy authentication.

Click the links below to see how Office 2013, Office 2016, and Office 2019 client authentication works with the Microsoft 365 services depending on whether or not modern authentication is turned on.

- [Exchange Online](#)
- [SharePoint Online](#)
- [Skype for Business Online](#)

Exchange Online

The following table describes the authentication behavior for Office 2013, Office 2016, and Office 2019 client apps when they connect to Exchange Online with or without modern authentication.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT (DEFAULT)	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT
Office 2019	No, AlwaysUseMSOAuth ForAutoDiscover = 1	Yes	Forces modern authentication on Outlook 2013, 2016, or 2019. More info	Forces modern authentication within the Outlook client.
Office 2019	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.
Office 2019	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.
Office 2019	Yes, EnableADAL=0	No	Basic authentication	Basic authentication
Office 2016	No, AlwaysUseMSOAuth ForAutoDiscover = 1	Yes	Forces modern authentication on 2013, 2016, or 2019. More info	Forces modern authentication within the Outlook client.
Office 2016	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT (DEFAULT)	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT
Office 2016	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.
Office 2016	Yes, EnableADAL=0	No	Basic authentication	Basic authentication
Office 2013	No	No	Basic authentication	Basic authentication
Office 2013	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then basic authentication is used. Server refuses modern authentication when the tenant is not enabled.

SharePoint Online

The following table describes the authentication behavior for Office 2013, Office 2016, and Office 2019 client apps when they connect to SharePoint Online with or without modern authentication.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT (DEFAULT)	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT
Office 2019	No, or EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2019	Yes, EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2019	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT (DEFAULT)	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT
Office 2016	No, or EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2016	Yes, EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.
Office 2016	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.
Office 2013	No	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.
Office 2013	Yes, EnableADAL = 1	Yes	Modern authentication only.	Failure to connect.

Skype for Business Online

The following table describes the authentication behavior for Office 2013, Office 2016, and Office 2019 client apps when they connect to Skype for Business Online with or without modern authentication.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT (DEFAULT)
Office 2019	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT (DEFAULT)
Office 2019	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.
Office 2019	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.
Office 2016	No, or EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.
Office 2016	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.
Office 2016	Yes, EnableADAL = 0	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.

OFFICE CLIENT APP VERSION	REGISTRY KEY PRESENT?	MODERN AUTHENTICATION ON?	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED ON FOR THE TENANT	AUTHENTICATION BEHAVIOR WITH MODERN AUTHENTICATION TURNED OFF FOR THE TENANT (DEFAULT)
Office 2013	No	No	Microsoft Online Sign-in Assistant only.	Microsoft Online Sign-in Assistant only.
Office 2013	Yes, EnableADAL = 1	Yes	Modern authentication is attempted first. If the server refuses a modern authentication connection, then Microsoft Online Sign-in Assistant is used. Server refuses modern authentication when Skype for Business Online tenants are not enabled.	Microsoft Online Sign-in Assistant only.

See also

[Enable Modern Authentication for Office 2013 on Windows devices](#)

[Multi-factor authentication for Microsoft 365](#)

[Sign in to Microsoft 365 with multi-factor authentication](#)

[Microsoft 365 Enterprise overview](#)

Microsoft 365 Isolation and Access Control in Azure Active Directory

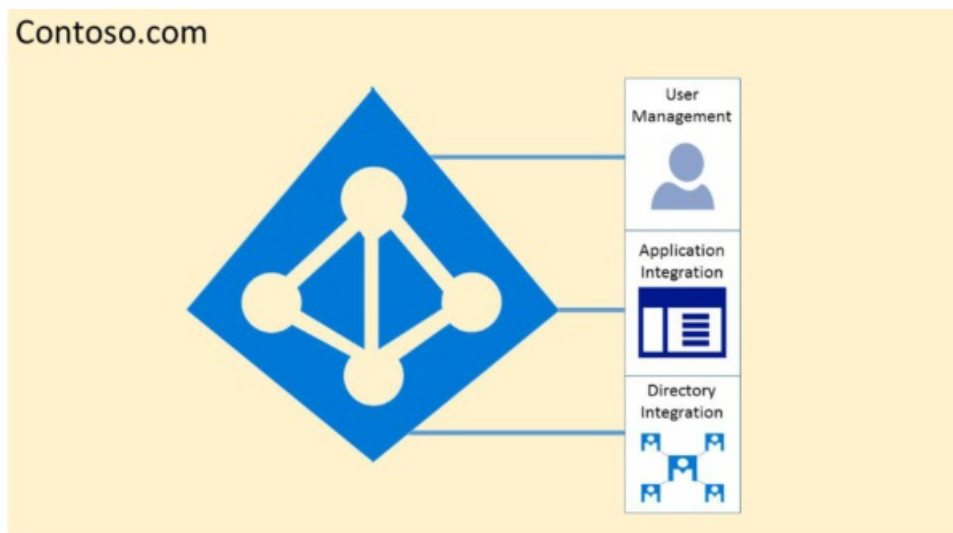
10/28/2022 • 2 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) was designed to host multiple tenants in a highly secure way through logical data isolation. Access to Azure AD is gated by an authorization layer. Azure AD isolates customers using tenant containers as security boundaries to safeguard a customer's content so that the content cannot be accessed or compromised by co-tenants. Three checks are performed by Azure AD's authorization layer:

- Is the principal enabled for access to Azure AD tenant?
- Is the principal enabled for access to data in this tenant?
- Is the principal's role in this tenant authorized for the type of data access requested?

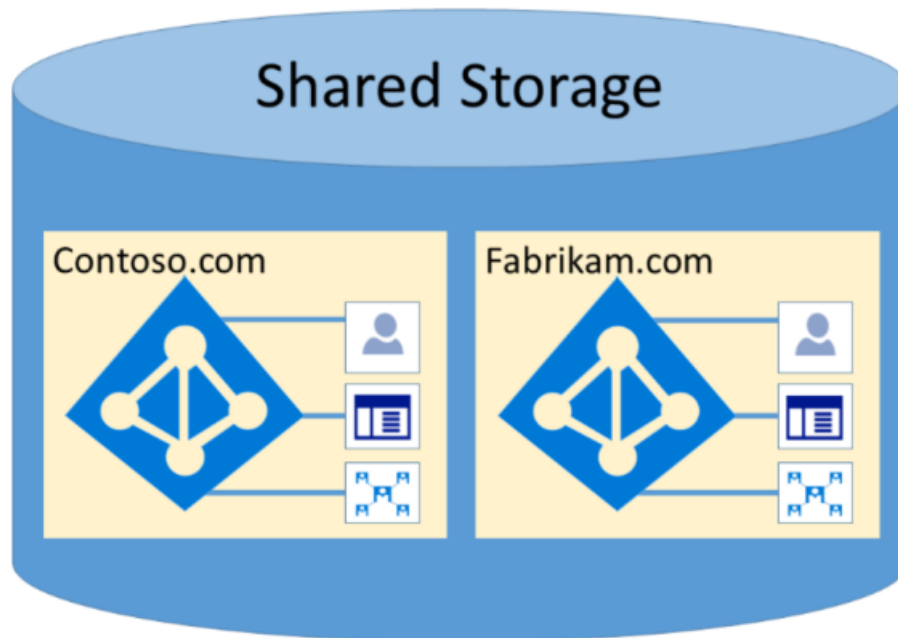
No application, user, server, or service can access Azure AD without the proper authentication and token or certificate. Requests are rejected if they are not accompanied by proper credentials.

Effectively, Azure AD hosts each tenant in its own protected container, with policies and permissions to and within the container solely owned and managed by the tenant.



The concept of tenant containers is deeply ingrained in the directory service at all layers, from portals all the way to persistent storage. Even when multiple Azure AD tenant metadata is stored on the same physical disk, there is no relationship between the containers other than what is defined by the directory service, which in turn is dictated by the tenant administrator. There can be no direct connections to Azure AD storage from any requesting application or service without first going through the authorization layer.

In the example below, Contoso and Fabrikam both have separate, dedicated containers, and even though those containers may share some of the same underlying infrastructure, such as servers and storage, they remain separate and isolated from each other, and gated by layers of authorization and access control.



In addition, there are no application components that can execute from within Azure AD, and it is not possible for one tenant to forcibly breach the integrity of another tenant, access encryption keys of another tenant, or read raw data from the server.

By default, Azure AD disallows all operations issued by identities in other tenants. Each tenant is logically isolated within Azure AD through claims-based access controls. Reads and writes of directory data are scoped to tenant containers, and gated by an internal abstraction layer and a role-based access control (RBAC) layer, which together enforce the tenant as the security boundary. Every directory data access request is processed by these layers and every access request in Microsoft 365 is policed by the logic above.

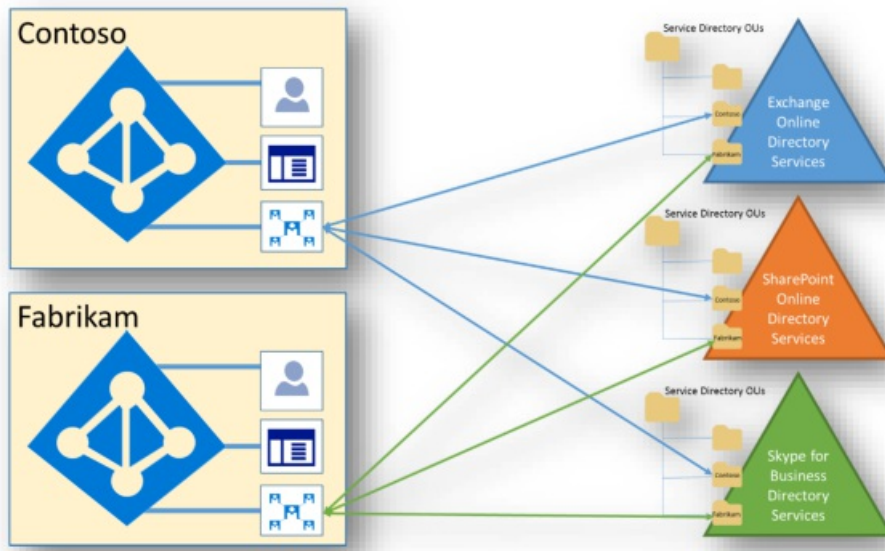
Azure AD has North America, U.S. Government, European Union, Germany, and World Wide partitions. A tenant exists in a single partition, and partitions can contain multiple tenants. Partition information is abstracted away from users. A given partition (including all the tenants within it) is replicated to multiple datacenters. The partition for a tenant is chosen based on properties of the tenant (e.g., the country code). Secrets and other sensitive information in each partition is encrypted with a dedicated key. The keys are generated automatically when a new partition is created.

Azure AD system functionalities are a unique instance to each user session. In addition, Azure AD uses encryption technologies to provide isolation of shared system resources at the network level to prevent unauthorized and unintended transfer of information.

Isolation and Access Control in Microsoft 365

10/28/2022 • 7 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) and Microsoft 365 use a highly complex data model that includes tens of services, hundreds of entities, thousands of relationships, and tens of thousands of attributes. At a high level, Azure AD and the service directories are the containers of tenants and recipients kept in sync using state-based replication protocols. In addition to the directory information held within Azure AD, each of the service workloads have their own directory services infrastructure.



Within this model, there's no single source of directory data. Specific systems own individual pieces of data, but no single system holds all the data. Microsoft 365 services cooperate with Azure AD in this data model. Azure AD is the "system of truth" for shared data, which is typically small and static data used by every service. The federated model used within Microsoft 365 and Azure AD provides the shared view of the data.

Microsoft 365 uses both physical storage and Azure cloud storage. Exchange Online (including Exchange Online Protection) and Skype for Business use their own storage for customer data. SharePoint Online uses both SQL Server storage and Azure Storage, hence the need for extra isolation of customer data at the storage level.

Exchange Online

Exchange Online stores customer data within mailboxes. Mailboxes are hosted within Extensible Storage Engine (ESE) databases called mailbox databases. This includes user mailboxes, linked mailboxes, shared mailboxes, and public folder mailboxes. User mailboxes include saved Skype for Business content, such as conversation histories.

User mailbox content includes:

- Emails and email attachments
- Calendaring and free/busy information
- Contacts
- Tasks
- Notes
- Groups
- Inference data

Each mailbox database within Exchange Online contains mailboxes from multiple tenants. An authorization code secures each mailbox, including within a tenancy. By default, only the assigned user has access to a mailbox. The access control list (ACL) that secures a mailbox contains an identity authenticated by Azure AD at the tenant level. The mailboxes for each tenant are limited to identities authenticated against the tenant's authentication provider, which includes only users from that tenant. Content in tenant A can't in any way be obtained by users in tenant B, unless explicitly approved by tenant A.

Skype for Business

Skype for Business stores data in various places:

- User and account information, which includes connection endpoints, tenant IDs, dial plans, roaming settings, presence state, contact lists, etc., is stored in the Skype for Business Active Directory servers, and in various Skype for Business database servers. Contact lists are stored in the user's Exchange Online mailbox if the user is enabled for both products, or on Skype for Business servers if the user isn't. Skype for Business database servers isn't partitioned per-tenant, but multi-tenancy isolation of data is enforced through Role-based access control (RBAC).
- Meeting content and uploaded-data is stored on Distributed File System (DFS) shares. This content can also be archived in Exchange Online if enabled. The DFS shares are not partitioned per-tenant. the content is secured with ACLs and multi-tenancy is enforced through RBAC.
- Call detail records, which are the activity history, such as call history, IM sessions, application sharing, IM history, etc., can also be stored in Exchange Online, but most call detail records are temporarily stored on call detail record (CDR) servers. Content isn't partitioned per tenant, but multi-tenancy is enforced through RBAC.

SharePoint Online

SharePoint Online has several independent mechanisms that provide data isolation. It stores objects as abstracted code within application databases. For example, when a user uploads a file to SharePoint Online, the file is disassembled, translated into application code, and stored in multiple tables across multiple databases.

If a user could gain direct access to the storage containing the data, the content isn't interpretable to a human or any system other than SharePoint Online. These mechanisms include security access control and properties. All SharePoint Online resources are secured by the authorization code and RBAC policy, including within a tenancy. The access control list (ACL) that secures a resource contains an identity authenticated at the tenant level. SharePoint Online data for a tenant is limited to identities authenticated by the authentication provider for the tenant.

In addition to the ACLs, a tenant level property that specifies the authentication provider (which is the tenant-specific Azure AD), is written once and can't be changed once set. Once the authentication provider tenant property has been set for a tenant, it cannot be changed using any APIs exposed to a tenant.

A unique *SubscriptionId* is used for each tenant. All customer sites are owned by a tenant and assigned a *SubscriptionId* unique to the tenant. The *SubscriptionId* property on a site is written once and is permanent. Once assigned to a tenant, a site can't be moved to a different tenant. The *SubscriptionId* is the key used to create the security scope for the authentication provider and is tied to the tenant.

SharePoint Online uses SQL Server and Azure Storage for content metadata storage. The partition key for the content store is *SiteId* in SQL. When running a SQL query, SharePoint Online uses a *SiteId* verified as part of a tenant-level *SubscriptionId* check.

SharePoint Online stores encrypted file content in Microsoft Azure blobs. Each SharePoint Online farm has its own Microsoft Azure account and all the blobs saved in Azure are encrypted individually with a key stored in the SQL content store. The encryption key protected in code by the authorization layer and not exposed directly to the end user. SharePoint Online has real-time monitoring to detect when an HTTP request reads or writes data

for more than one tenant. The request identity *SubscriptionId* is tracked against the *SubscriptionId* of the accessed resource. Requests to access resources of more than one tenant should never happen by end users. Service requests in a multi-tenant environment are the only exception. For example, the search crawler pulls content changes for an entire database all at once. This usually involves querying sites of more than one tenant in a single service request, which is done for efficiency reasons.

Teams

Your Teams data is stored differently, depending on the content type.

Check out the [Ignite breakout session on Microsoft Teams architecture](#) for an in-depth discussion.

Core Teams customer data

If your tenant is provisioned in Australia, Canada, the European Union, France, Germany, India, Japan, South Africa, South Korea, Switzerland (which includes Liechtenstein), the United Arab Emirates, the United Kingdom, or the United States, Microsoft stores the following customer data at rest only within that location:

- Teams chats, team and channel conversations, images, voicemail messages, and contacts.
- SharePoint Online site content and the files stored within that site.
- Files uploaded to OneDrive for work or school.

Chat, channel messages, team structure

Every team in Teams is backed by a Microsoft 365 Group and its SharePoint site and Exchange mailbox. Private chats (including group chats), messages sent as part of a conversation in a channel, and the structure of teams and channels are stored in a chat service running in Azure. The data is also stored in a hidden folder in the user and group mailboxes to enable Information Protection features.

Voicemail and contacts

Voicemails are stored in Exchange. Contacts are stored in Exchange-based cloud data store. Exchange and the Exchange-based cloud store already provide data residency in each of the worldwide datacenter geos. For all teams, voicemail and contacts are stored in-country for Australia, Canada, France, Germany, India, Japan, the United Arab Emirates, the United Kingdom, South Africa, South Korea, Switzerland (which includes Liechtenstein), and the United States. For all other countries, files are stored in the US, Europe, or Asia-Pacific location based on tenant affinity.

Images and media

Media used in chats (except for Giphy GIFs that aren't stored but are a reference link to the original Giphy service URL, Giphy is a non-Microsoft service) is stored in an Azure-based media service that is deployed to the same locations as the chat service.

Files

Files (including OneNote and Wiki) that somebody shares in a channel are stored in the team's SharePoint site. Files shared in a private chat or a chat during a meeting or call are uploaded and stored in the OneDrive for work or school account of the user who shares the file. Exchange, SharePoint, and OneDrive already provide data residency in each of the worldwide datacenter geos. So, for existing customers, all files, OneNote notebooks, Teams wiki content, and mailboxes that are part of the Teams experience are already stored in the location based on your tenant affinity. Files are stored in-country for Australia, Canada, France, Germany, India, Japan, the United Arab Emirates, the United Kingdom, South Africa, South Korea, and Switzerland (which includes Liechtenstein). For all other countries, files are stored in the US, Europe, or Asia Pacific location based on tenant affinity.

Add a domain to Microsoft 365

10/28/2022 • 5 minutes to read • [Edit Online](#)

[Check the Domains FAQ](#) if you don't find what you're looking for.

Check out [Microsoft 365 small business help](#) on YouTube.

Before you begin

To add, modify, or remove domains, you **must** be a **Domain Name Administrator** or **Global Administrator** of a [business or enterprise plan](#). These changes affect the whole tenant; *Customized administrators* or *regular users* won't be able to make these changes.

TIP

If you need help with the steps in this topic, consider [working with a Microsoft small business specialist](#). With Business Assist, you and your employees get around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use.

Watch: Add a domain

Check out this video and others on our [YouTube channel](#).

Your company might need multiple domain names for different purposes. For example, you might want to add a different spelling of your company name because customers are already using it and their communications have failed to reach you.

1. In the Microsoft 365 admin center, choose **Setup**.
2. Under **Get your custom domain set up**, select **View** > **Manage** > **Add domain**.
3. Enter the new domain name that you want to add, and then select **Next**.
4. Sign in to your domain registrar, and then select **Next**.
5. Choose the services for your new domain.
6. Select **Next** > **Authorize** > **Next**, and then **Finish**. Your new domain has been added.

Add a domain

Follow these steps to add, set up, or continue setting up a domain.

1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to the **Settings** > **Domains** page.
3. Select **Add domain**.
4. Enter the name of the domain you want to add, then select **Next**.
5. Choose how you want to verify that you own the domain.
 - a. If your domain registrar uses [Domain Connect](#), Microsoft [will set up your records automatically](#) by

having you sign in to your registrar and confirm the connection to Microsoft 365. You'll be returned to the admin center and Microsoft will then automatically verify your domain.

- b. You can use a TXT record to verify your domain. Select this and select **Next** to see instructions for how to add this DNS record to your registrar's website. This can take up to 30 minutes to verify after you've added the record.

- c. You can add a text file to your domain's website. Select and download the .txt file from the setup wizard, then upload the file to your website's top level folder. The path to the file should look similar to:

`http://mydomain.com/ms39978200.txt`. We'll confirm you own the domain by finding the file on your website.

- 6. Choose how you want to make the DNS changes required for Microsoft to use your domain.

- a. Choose **Add the DNS records for me** if your registrar supports [Domain Connect](#), and Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365.
- b. Choose **I'll add the DNS records myself** if you want to attach only specific Microsoft 365 services to your domain or if you want to skip this for now and do this later. **Choose this option if you know exactly what you're doing.**

- 7. If you chose to *add DNS records yourself*, select **Next** and you'll see a page with all the records that you need to add to your registrar's website to set up your domain.

If the portal doesn't recognize your registrar, you can [follow these general instructions](#).

If you don't know the DNS hosting provider or domain registrar for your domain, see [Find your domain registrar or DNS hosting provider](#).

If you want to wait for later, either unselect all the services and click **Continue**, or in the previous domain connection step choose **More Options** and select **Skip this for now**.

- 8. Select **Finish** - you're done!

Add or edit custom DNS records

Follow the steps below to add a custom record for a website or 3rd party service.

1. Sign in to the Microsoft admin center at <https://admin.microsoft.com>.
2. Go to the **Settings > Domains** page.
3. On the **Domains** page, select a domain.
4. Under **DNS settings**, select **Custom Records**; then select **New custom record**.
5. Select the type of DNS record you want to add and type the information for the new record.
6. Select **Save**.

Registrars with Domain Connect

[Domain Connect](#) enabled registrars let you add your domain to Microsoft 365 in a three-step process that takes minutes.

In the wizard, we'll just confirm that you own the domain, and then automatically set up your domain's records, so email comes to Microsoft 365 and other Microsoft 365 services, like Teams, work with your domain.

NOTE

Make sure you disable any popup blockers in your browser before you start the setup wizard.

Domain Connect registrars integrating with Microsoft 365

- [1&1 IONOS](#)
- [EuroDNS](#)
- [Cloudflare](#)
- [GoDaddy](#)
- [WordPress.com](#)
- [Plesk](#)
- [MediaTemple](#)
- SecureServer or WildWestDomains (GoDaddy resellers using SecureServer DNS hosting)
 - Examples:
 - [DomainsPricedRight](#)
 - [DomainRightNow](#)

What happens to my email and website?

After you finish setup, the MX record for your domain is updated to point to Microsoft 365 and all email for your domain will start coming to Microsoft 365. Make sure you've added users and set up mailboxes in Microsoft 365 for everyone who gets email on your domain!

If you have a website that you use with your business, it will keep working where it is. The Domain Connect setup steps don't affect your website.

Add an onmicrosoft.com domain

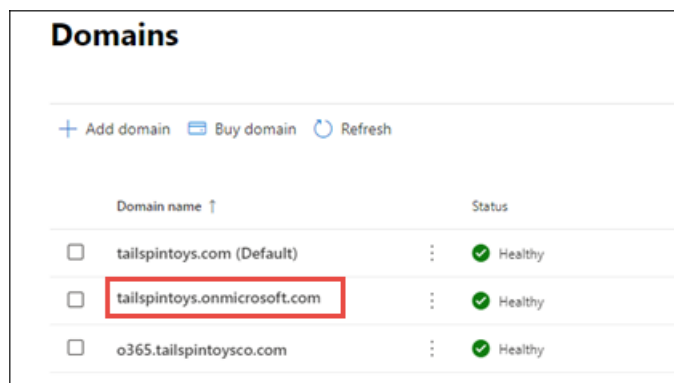
Each Microsoft 365 organization can have up to five onmicrosoft.com domains.

NOTE

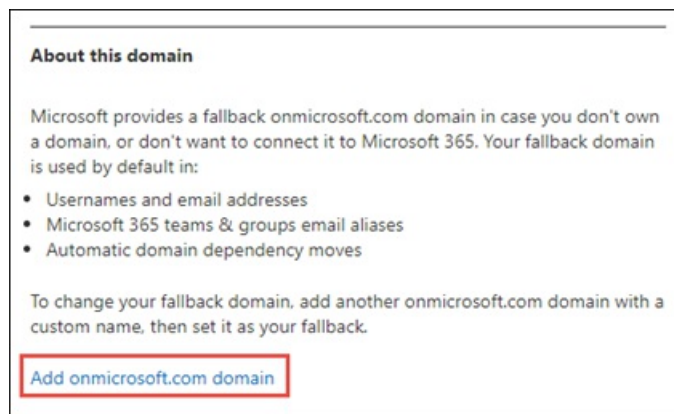
You must be a Global admin or a Domain Name admin to add a domain. Creating an additional .onmicrosoft domain and using it as your default will not do a rename for SharePoint Online. To make changes to your .onmicrosoft SharePoint domain you would need to use the [SharePoint domain rename preview](#) (currently available to any tenant with less than 10,000 sites). If you're using Microsoft 365 mail services, removal of your initial .onmicrosoft domain is not supported.

To add an onmicrosoft.com domain:

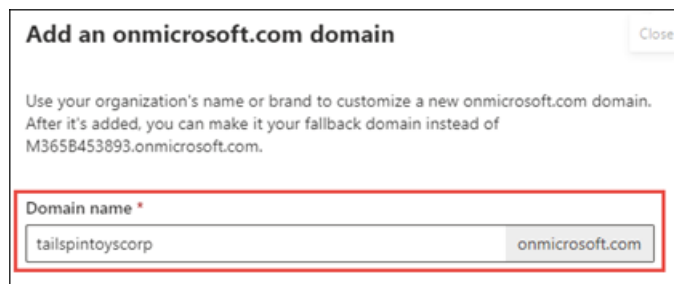
1. In the Microsoft 365 admin center, select **Settings**, and then select **Domains**.
2. Select an existing *.onmicrosoft.com* domain.



3. On the **Overview** tab, select **Add onmicrosoft.com domain**.



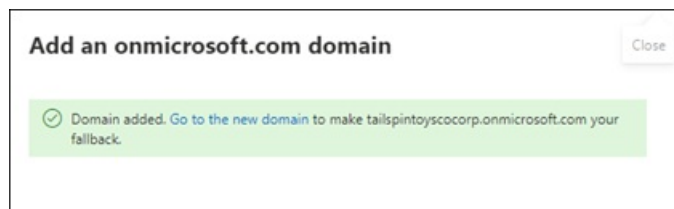
4. On the **Add onmicrosoft domain** page, in the **Domain name** box, enter the name for your new onmicrosoft.com domain.



NOTE

Make sure to verify the spelling and accuracy of the domain name you entered. You are limited to five onmicrosoft.com domains, and currently they cannot be deleted once they are created.

5. Select **Add domain**. When successfully added, you will see a message stating this.



You can set any domain you own as your default domain.

For more details on how to add an onmicrosoft.com domain, see [Add or replace your onmicrosoft.com domain](#).

Related content

[Domains FAQ](#) (article)

[What is a domain?](#) (article)

[Buy a domain name in Microsoft 365](#) (article)

[Add DNS records to connect your domain](#) (article)

[Change nameservers to set up Microsoft 365 with any domain registrar](#) (article)

Microsoft 365 network health status

10/28/2022 • 2 minutes to read • [Edit Online](#)

Due to the increased demand for Microsoft's cloud services during the COVID-19 crisis, we are providing information about the health of Microsoft's global network and information about network quality issues that our customers might experience but that we don't control.

This information includes network issues that affect all of our software as service offerings, including Microsoft 365.

There might be delays in the updates to this page. We are updating it manually while we build a more automated solution.

When we detect significant issues within Microsoft's global network or with internet connectivity between our customers and Microsoft's network, we'll post that information here. We recommend that customers continue to use the Microsoft 365 admin center [Service Health dashboard](#) to understand the impact of any significant network issues on their tenant, as we provide much more detailed and targeted information there.

Current network issues

LOCATION	ISSUE TYPE	DETAIL
No current issues		

Recommendations to improve network experience

Use these resources to improve your network utilization for Microsoft services.

- [Optimize Microsoft 365 connectivity for remote users using VPN split tunneling](#)
- [Microsoft 365 principles of network connectivity](#)
- [Working remotely using Azure Networking services](#)

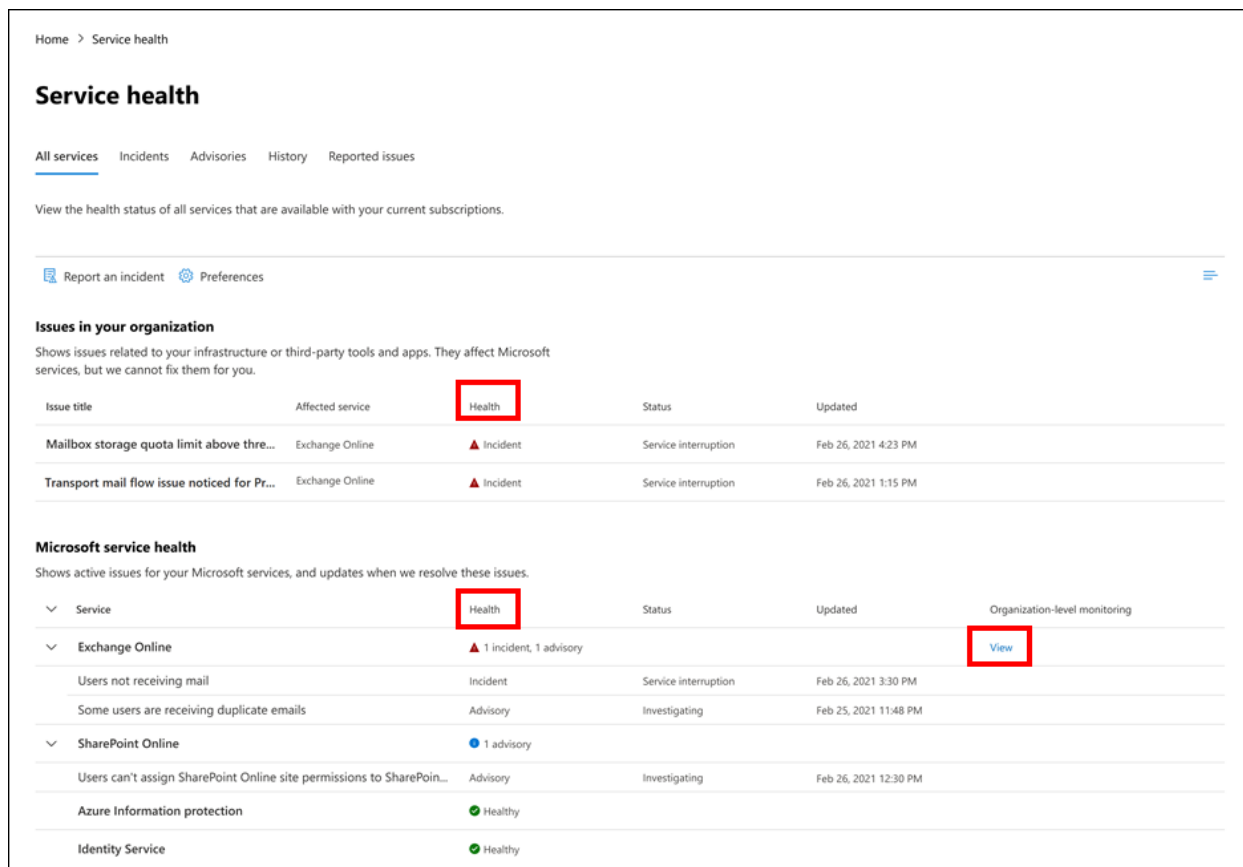
Learn about Microsoft 365 monitoring

10/28/2022 • 4 minutes to read • [Edit Online](#)

You can use dashboards in the [Microsoft 365 admin center](#) to monitor the health of various Microsoft services for your organization's Microsoft 365 subscription. This capability was initially started with Exchange Online and now getting expanded to other Microsoft services like Microsoft Teams, Microsoft 365 Apps and more service in future. Monitoring provides you with information about incidents and advisories that are collected in these categories:

- **Infrastructure.** Issue is detected in the Microsoft 365 infrastructure that Microsoft owns for providing regular updates and resolving the issue. For example, users can't access Exchange Online because of issues with Exchange or other Microsoft 365 cloud infrastructure.
- **Third-party infrastructure.** Issue is detected in third-party infrastructure on which your organization has taken a dependency and requires action from your organization for resolution. For example, user authentication transactions are getting throttled by a third-party security token service (STS) provider that prevents users from connecting to Exchange Online.
- **Customer infrastructure.** Issue is detected in your organization's infrastructure and requires action from your organization for resolution. For example, users can't access Exchange Online because they are unable to obtain an authentication token from STS provider hosted by your organization because of an expired certificate.

Here's an example of the **Service health** page in the Microsoft 365 admin center, which is available at **Health > Service health** for organization scenarios and [priority account](#) scenarios.



Home > Service health

Service health

All services Incidents Advisories History Reported issues

View the health status of all services that are available with your current subscriptions.

[Report an incident](#) [Preferences](#)

Issues in your organization

Shows issues related to your infrastructure or third-party tools and apps. They affect Microsoft services, but we cannot fix them for you.

Issue title	Affected service	Health	Status	Updated
Mailbox storage quota limit above thre...	Exchange Online	▲ Incident	Service interruption	Feb 26, 2021 4:23 PM
Transport mail flow issue noticed for Pr...	Exchange Online	▲ Incident	Service interruption	Feb 26, 2021 1:15 PM

Microsoft service health

Shows active issues for your Microsoft services, and updates when we resolve these issues.

Service	Health	Status	Updated	Organization-level monitoring
Exchange Online	▲ 1 incident, 1 advisory			View
Users not receiving mail	Incident	Service interruption	Feb 26, 2021 3:30 PM	
Some users are receiving duplicate emails	Advisory	Investigating	Feb 25, 2021 11:48 PM	
SharePoint Online	● 1 advisory			
Users can't assign SharePoint Online site permissions to SharePoin...	Advisory	Investigating	Feb 26, 2021 12:30 PM	
Azure Information protection	● Healthy			
Identity Service	● Healthy			

Issues in your organization will be identified and used by organizational-level monitoring and priority account monitoring.

The value of the **Health** column under **Issues in your organization** indicates whether your organization's infrastructure or third-party software affects the service health experience of your organization's users and/or priority accounts in Exchange Online. Advisories or incidents require your actions to resolve.

The value of the **Health** column under **Microsoft service health** indicates that the service is healthy or has advisories or incidents based on the cloud services that Microsoft maintains.

Here's an example of the Exchange Online monitoring page in the Microsoft 365 admin center that shows the health of organization-level and priority account scenarios available from **Health > Service health > Exchange Online**.

Exchange Online				
We monitor Exchange Online for Microsoft 365 service issues, as well as infrastructure and third-party software issues that might require your action.				
Scenarios Active issues				
Organization scenarios				
App and activities	Health	Action required	Activity (last 30 min)	Change in activity (last 7 days)
App connectivity	Healthy	No	99.581% estimated connectivity	0% change
Basic authentication	Healthy	No	25 authentications	+32% change
Desktop mail apps	Healthy	No	30,524 users read mail	+5% change
iOS and Android mail apps	Healthy	No	3,520 users read mail	+4% change
Mail delivery	Healthy	No	659,528 messages delivered	-14% change
Modern authentication	Healthy	No	12,329 authentications	+28% change
Open Outlook on the web	Healthy	No	228 users opened app	-57% change
Outlook apps for Mac	Healthy	No	939 users read mail	+28% change
Outlook apps for mobile	Healthy	No	6,389 users read mail	-6% change
Outlook on the web	Healthy	No		

With the scenario list page, you can see whether the Microsoft service is healthy or not and whether there are any associated incidents or advisories. For example, with Exchange Online monitoring, you can look at the service health for specific email scenarios and view near real-time signals to determine the impact by organization-level scenario. You can also see health of priority account scenarios, if available.

Requirements for monitoring

This preview is enabled for customers who meet the following requirements:

- Your organization needs to have a license count of at least 5,000 from one or a combination of these products: Office 365 E3, Microsoft 365 E3, Office 365 E5, or Microsoft 365 E5.

For example, your organization can have 3,000 Office 365 E3 licenses and 2,500 Microsoft 365 E5, for a total of 5,500 licenses from the qualifying products.

- Your organization needs to have at least 50 monthly active users for one or more core Microsoft 365 services, which include Microsoft Teams, OneDrive for Business, SharePoint Online, Exchange Online, and Office apps.
- Any role with Service Health Dashboard level permissions can access Exchange Online Monitoring. For more information, see [How to check Microsoft 365 service health](#).

Additional monitoring for Microsoft services

Service-specific monitoring is also enable for the following Microsoft services. Select the corresponding link to learn more about monitoring for that service.

- [Exchange Online](#)

- [Microsoft 365 Apps](#)
- [Microsoft Teams](#)

Send us feedback

There are two ways you can provide feedback:

- Use the **Give feedback** option available on every page of the Microsoft 365 admin center.
- Submit feedback using the **Is this post helpful?** link for a specific incident or advisory.

Users unable to send emails

EXT43260, Exchange Online, Last updated: December 19, 2016 6:00 AM
Start time: May 18, 2016 2:02 AM

Status
Service interruption

Issue type	Issue origin
▲ Incident	Microsoft

User impact
A large number of customers appear to be impacted by this event. We've received a few isolated customer reports of this issue.

[Are you experiencing this issue?](#)
[Is this post helpful?](#)

Latest message, July 8, 2016 2:05 AM [View history](#)

The Office 365 Suite team is investigating a possible issue impacting acquisition of data from blog sources. If this is affecting you, we apologize for the inconvenience. Message 2.

Frequently asked questions

1. Why don't I see "view" link under Organizational monitoring column in the Microsoft 365 admin center inside Service Health?

First, make sure you've enabled the new admin center on the **Home** page of the [Microsoft 365 admin center](#).

Then make sure you meet both of the following requirements:

- Your organization needs to have a license count of at least 5,000, from one or a combination of these products: Office 365 E3, Microsoft 365 E3, Office 365 E5, or Microsoft 365 E5.
- Your organization needs to have at least 50 monthly active users for one or more core Microsoft 365 services, which include Microsoft Teams, OneDrive for Business, SharePoint Online, Exchange Online, and Office apps.

If the license count for your organization falls below 5,000 users and the monthly active users falls below 50 users in the core services, Exchange Online monitoring won't be enabled until these requirements are met.

2. Will there be other monitoring scenarios for other services in future?

Yes. We have a few more services in public preview now. We'll continue to work on expanding the footprint to other services.

3. What is the plan for general availability of this experience?

Microsoft's plan is to collect your feedback on the preview experience and then define our plan for general availability.

4. Is this a free (included) or paid (extra) feature?

This is a free feature that is in preview and only available for customers that meet the requirements in question

1. There isn't a paid option to receive this content.

5. How do I provide feedback?

For general feedback, use the **Give feedback** icon on the bottom-right corner of the monitoring page.

For feedback on incidents or advisories, use the ****Is this post helpful?** link.

6. Are there any privacy concerns?

Monitoring focuses on service metadata and user content isn't monitored.

Exchange Online monitoring for Microsoft 365

10/28/2022 • 3 minutes to read • [Edit Online](#)

Exchange Online monitoring supports the following organization-level scenarios:

- **Email clients:** You can view the health for the following email clients based on email read activity:
 - Outlook desktop
 - Outlook on the web
 - Native mail clients of iOS and Android
 - Outlook Mobile app in iOS and Android
 - Outlook Mac client

For these clients, you can see the number of active users in the last 30 minutes based on users reading an email, along with number of incidents and advisories in the dashboard. This data is compared to the same interval for the previous week to see if there's an issue.

NOTE

Active user count is measured by a single activity, for example, when a user reads an email. It only accounts for the last 30 minutes of activity.

- **App connectivity:** Estimated connectivity is based on the percentage of successful, synthetic connections between your organization's devices and Exchange Online, and may include issues outside of Microsoft's control. To learn more, see [Microsoft 365 Connectivity Optics](#).
- **Basic Authentication and Modern Authentication:** The number of users successfully validated in the Exchange Online service.
- **Mail flow:** The number of messages successfully delivered to a mailbox without any delay after the message reached the Microsoft 365 network.
- **Open Outlook for the Web:** The number of users successfully signed in and started Outlook on the web.

Here's an example of the organization-level scenarios for Exchange Online in the main dashboard.

Exchange Online

We monitor Exchange Online for Microsoft 365 service issues, as well as infrastructure and third-party software issues that might require your action.

[Scenarios](#) [Active issues](#)

Organization scenarios

App and activities	Health ↑	Action required	Activity (last 30 min)	Change in activity (last 7 days)
App connectivity	🟢 Healthy	No	99.581% estimated connectivity	0% change
Basic authentication	🟢 Healthy	No	25 authentications	+32% change
Desktop mail apps	🟢 Healthy	No	30,524 users read mail	+5% change
iOS and Android mail apps	🟢 Healthy	No	3,520 users read mail	+4% change
Mail delivery	🟢 Healthy	No	659,528 messages delivered	-14% change
Modern authentication	🟢 Healthy	No	12,329 authentications	+28% change
Open Outlook on the web	🟢 Healthy	No	228 users opened app	-57% change
Outlook apps for Mac	🟢 Healthy	No	939 users read mail	+28% change
Outlook apps for mobile	🟢 Healthy	No	6,389 users read mail	-6% change
Outlook on the web	🟢 Healthy	No		

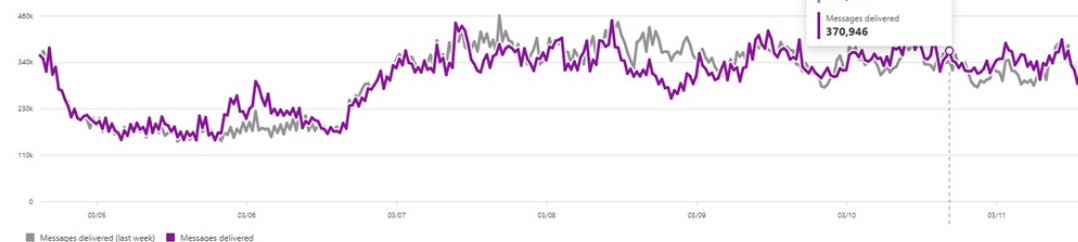
For these scenarios, the key numbers are for the last 30 minutes in the main dashboard. Detailed views for each of these scenarios show the near real-time trend for seven days with the 30-minute aggregate compared with the previous week.

Mail delivery

Messages successfully delivered

Success is based on message delivery within 15 minutes of its receipt by Exchange Online. Data is shown at 30-minute intervals. All data is for the past 7 days, except for the line labeled "Messages delivered (last week)."

Updated 2:29 PM PST



Active issues (0)

Issue title	Issue type	Status ↑	Action required	Issue origin	ID	Start time	Last updated
-------------	------------	----------	-----------------	--------------	----	------------	--------------

You'll notice incidents or advisories created for your organization with "Issue origin" in the communication tagged as "Your org". These are notifications individually targeted to your organization with issues that require your attention for mitigation and resolution. For more information about various types of issues that are created and communicated in service health to inform your organization about the potential impact, see the following articles:

- [Service alerts for mailbox utilization](#)
- [Service alerts for MRS source delays](#)
- [Service alerts for messages pending delivery to external recipients](#)

Priority accounts monitoring scenarios

With Exchange Online priority account monitoring, you can view the health for the following scenarios after configuring [priority accounts](#):

- Exchange licensing

- Mailbox storage
- Message limit
- Subfolders per folder
- Folder hierarchy
- Recoverable items

The Exchange licensing scenario checks if the priority account isn't able to log in due to invalid license issues, which can be addressed by the tenant admin.

The remaining five scenarios above check if your priority account's mailbox is close to reaching or has reached the limits described in [Exchange Online limits](#).

For these scenarios, you can see active and resolved advisories and incidents affecting your priority accounts. Identifiable information for the priority accounts will be displayed in the advisory or incident details along with recommendations. Here's an example from the page at **Health > Service health > Exchange Online**.

Priority account scenarios		
App and activities	Health ↑	Action required
Exchange licensing	✓ Healthy	No
Folder hierarchy	✓ Healthy	No
Mailbox storage	✓ Healthy	No
Message limit	✓ Healthy	No
Recoverable items	✓ Healthy	No
Subfolders per folder	✓ Healthy	No

In the affected account pane, the **Status** column has these values:

- Fixed: The issue causing the advisory or incident has been addressed for the priority account. There's no longer an issue.
- Active: The issue causing the advisory or incident is ongoing for the priority account. The issue remains.
- Delayed: The issue causing the advisory or incident hasn't been addressed for the priority account in 96 hours, so it's suspended. The issue remains.

Here's an example.

Home > Service health > Exchange Online > Mailbox storage

Mailbox storage

All active issues (1)

Issue title	Issue type	Status	Requires your action?	Issue origin	ID
Mailbox storage quota limit above threshold	▲ Incident	Service interruption	Yes	Your org	EX0

Resolved issues, past 7 days (1)

Issue title	Issue type	Status	Issue origin	ID
Mailboxes over storage limit	▲ Incident	Service restored	Your org	EX0

N affected accounts

Incident: Mailboxes over storage limit

Export<# items>

Display name	Username	Status ↑	Usage
Michael Scott	michaelscott@contoso.co...	Active	100%
Dwight Schrute	dwightschrute@contoso.co...	Fixed	100%
Jane Doe	janedoe@contoso.co...	Delayed	100%

An advisory or incident will be resolved after no accounts remain in the **Active** state.

Frequently asked questions

1. The active user count in the dashboard for each client appears to be low. We have a lot of active licenses assigned to users. What does this mean?

The active user count shown in monitoring is based on a 30-minute window where users have performed the activity called out in the feature. This shouldn't be confused with usage numbers. To view usage numbers, use activity reports in the Microsoft 365 admin center (**Reports** > [Usage](#)).

2. Where is the data instrumented for the scenarios that show activity trends?

The data is instrumented in the Exchange Online service. If there's a failure that happens before the request reaches Exchange Online or there's a failure in Exchange Online, you'll see a drop in the activity signal.

Service advisories for mailbox utilization in Exchange Online monitoring

10/28/2022 • 7 minutes to read • [Edit Online](#)

We've released a new Exchange Online service advisory that informs you of mailboxes that are on hold that are at risk of reaching or exceeding their quota. These service advisories provide visibility to the number of mailboxes in your organization that may require admin intervention.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to **Health > Service health > Exchange Online** and then click the **Active issues** tab. Here's an example of a mailbox utilization service advisory.

Exchange Online							
We monitor Exchange online for Microsoft 365 issues, as well as infrastructure and third-party software issues that might require your action.							
Scenarios		Active Issues					
Title	Issue type	Requires customer action?	Issue origin	Status	ID	Start time	Last updated
Microsoft has detected a number of mailboxes that have exceeded or are at risk of reaching their quota limits.	Advisory	Yes	Your Org	Investigating	EX275752	Aug 5, 2021 7:47 AM	Aug 5, 2021 7:54 AM

To display a list of mailboxes that are nearing their storage quota, select the highlighted link in the following screenshot to access your mailbox usage report. This link is displayed in the service advisory.

The following table provides an overview of at utilization risk mailboxes assigned per Retention Policy in your environment. For mailboxes with an archive, if no Recoverable Item Tags or MoveToArchive tag is created then content will not move automatically (unless a personal tag is assigned or dumpster content is older than 30 days).	
Please refer to aka.ms/MailboxUsagePortal for detailed mailbox usage data to determine which mailboxes are close to and over the quota.	
Please refer to aka.ms/MailboxFolderLimits for guidance around Exchange Online limits.	
Please refer to aka.ms/MessageRecordsMgmt for guidance around configuring compliance policies in your organization.	
Please refer to aka.ms/MailboxReachesQuota for guidance if a mailbox reaches its quota limit even if the Archive feature is enabled.	
Please refer to aka.ms/MailboxFullWarning for guidance if a mailbox receives a 'Mailbox is Full' warning even if the mailbox hasn't reached its storage limit.	

Alternatively, the direct URL to the mailbox usage report is <https://admin.microsoft.com/Adminportal/Home?source=applauncher#/reportsUsage/MailboxUsage>.

NOTE

The mailbox usage report information could be 24 hours behind your mailbox utilization service advisory alert.

What do these service advisories indicate?

The service advisories for mailbox utilization inform admins about mailboxes on hold that are nearing the mailbox storage quota. The type of holds that that can be placed on mailboxes include Litigation holds, eDiscovery hold, and Microsoft 365 retention policies (that are configured to retain data). When a mailbox is on hold, users (or automated processes) can't permanently remove data from their mailbox. Instead, admins must configure MRM retention policies in Exchange Online (inline with their organization's compliance policies related to data retention) to move data from a user's primary mailbox to their archive mailbox. If not and a mailbox on a hold reaches a critical or warning state, admins have to [enable archive mailboxes](#) and [enable auto-expanding archiving](#) and then make sure that the retention period for the archive policy assigned to the mailbox (that moves email from the primary mailbox to the archive mailbox) is short enough. If nothing is done to resolve the quota issues that are identified by the mailbox utilization service advisory, then users might not be able to send or receive email messages or meeting invites.

A service advisory for mailbox utilization contains tables about the number of mailboxes that are nearing their quota. The following sections describe the information in these tables and the action admins can take to help ensure these mailboxes don't exceed their quota.

NOTE

Service advisories contain descriptions of the mailbox quota properties that appear in the columns in the tables described in the following sections.

Mailboxes on hold without an archive

The following table lists the number of mailboxes on hold that are nearing their quota but don't have an archive mailbox enabled. Each column in the table identifies the specific quota and the number of mailboxes nearing that quota.

# MAILBOXES PROHIBITSENDRECEIVEQUOTA (WARNING)	# MAILBOXES PROHIBITSENDRECEIVEQUOTA (CRITICAL)**	# MAILBOXES RECOVERABLEITEMSQUOTA (WARNING)	# MAILBOXES RECOVERABLEITEMSQUOTA (CRITICAL)**
2	2	1	0

The action admins can take for these mailboxes is to enable the archive mailbox and ensure that an MRM archive policy (which is an MRM retention policy in Exchange Online that moves items to the archive mailbox) is applied to the mailbox so that items are moved to the archive mailbox. For more information, see [Set up an archive and deletion policy for mailboxes](#).

After you enable an archive mailbox, we recommend that you consider increasing the quota for the Recoverable Items folder. This helps prevent exceeding the quota for the Recoverable Items folder for mailboxes that are placed on hold. For more information, see [Increase the Recoverable Items quota for mailboxes on hold](#).

Mailboxes on hold with an archive

The following table lists the number of mailboxes on hold that are nearing their quota and have an archive mailbox enabled.

# MAILBOXES PROHIBITSENDRECEIVEQUOTA (WARNING)	# MAILBOXES PROHIBITSENDRECEIVEQUOTA (CRITICAL)	# MAILBOXES RECOVERABLEITEMSQUOTA (WARNING)	# MAILBOXES RECOVERABLEITEMSQUOTA (CRITICAL)**
1	1	6	0

The action admins can take for these mailboxes is to increase the quota for the Recoverable Items folder. For more information, see [Increase the Recoverable Items quota for mailboxes on hold](#).

Admins should also make sure that an MRM archive policy that moves items to the archive mailbox is also applied to the mailboxes, and that the retention period for the archive policy is short enough so that items aren't retained too long in the primary mailbox before they're moved to the archive.

NOTE

MRM archive policies also move items from the Recoverable Items folder in the primary mailbox to the Recoverable Items folder in the corresponding archive mailbox. This capability helps prevent the mailbox from exceeding the quota for the Recoverable Items quota.

MRM retention policies in your organization

Service advisories for mailbox utilization may also contain a table with information about the MRM retention policies in your organization and whether or not the mailboxes that are a retention policy have an archive mailbox. For more information about retention policies, see [Retention tags and retention policies in Exchange Online](#).

RETENTIONPOLICYGUID	MAILBOXTYPE	HASMOVEDUMPSTERTOARCHIVETAG	HASMOVEPRIMARYTOARCHIVETAG	HASPERSONALARCHIVETAG	MAILBOXES
6c041498-1611-5011-a058-1156ce60890c	PrimaryWithArchive	True	False	True	398
6c041498-1611-5011-a058-1156ce60890c	Primary	True	False	True	10
749ceecc-d49d-4000-a9d5-594dbaea1e56	PrimaryWithArchive	False	True	False	7
269f6a85-1234-4648-8cde-59bbc7bc67d0	PrimaryWithArchive	True	True	True	1
13fb778d-e1cb-4c44-5768-ad4282906c1f	PrimaryWithArchive	True	True	False	1

The following list describes each column in the previous table.

- **RetentionPolicyGuid:** The GUID of the retention policy assigned to mailboxes in your organization. In the previous example, there are two separate rows for the same retention policy. The first row indicates the number of mailboxes with an archive that are assigned the policy. The second row indicates the number of mailboxes without an archive that are assigned the same policy.

To obtain more information about the retention policy listed in this column, run the following command in [Exchange Online PowerShell](#).

```
Get-RetentionPolicy <GUID> | FL
```

The value of the **Name** property is the name of the retention policy that's displayed on the **Retention policies** page in the [Exchange admin center](#).

- **MailboxType:** Specifies what type of mailboxes the policy is assigned to. Values include *Primary* (mailboxes without an archive) or *PrimaryWithArchive* (mailboxes with an archive). If the value in this column is *Primary*, then you should enable the archive for the mailboxes (the **Mailbox** column indicates the number of these mailboxes) that are assigned the policy. Otherwise, an archive policy or personal archive tag won't work because there isn't an archive to move items to.
- **HasMoveDumpsterToArchiveTag:** Indicates that the retention policy includes a retention tag that move items in the Recoverable Items folder (also called the *dumpster*) in the primary mailbox to the Recoverable Items folder in the archive. This type of retention tag is set by an admin. If the retention period for the recoverable items tag is too long, then reducing the retention period should help prevent

mailboxes from nearing the quota for Recoverable Items folder. For example, if the retention period is set to 30 days, reducing it to three or five days may help. For more information, see [Increase the Recoverable Items quota for mailboxes on hold](#).

- **HasMovePrimaryToArchiveTag:** Indicates if there is a default "move to archive" retention tag (also called an *archive policy*) included in the retention policy. In this case, messages will be moved from the regular folders in the primary mailbox to the archive mailbox. This type of retention tag is set by an admin. Again, if the retention period for this tag is too short, users may have problems with continually reaching the quota for their primary mailbox. Reducing the retention period for an archive policy may help solve this issue.
- **HasPersonalArchiveTag:** Indicates if the retention policy includes a personal "move to archive" tag. If the retention policy does include a personal "move to archive" tag, then users can apply this tag to folders and messages in their mailbox to move items to the archive. Users can also set up an inbox rule to move messages to a folder with this tagged applied to it. In both cases, this can help move items to the archive to help avoid reaching the quota for their primary mailbox.
- **Mailboxes:** Indicates the number of mailboxes (those with or without an archive, which is indicated in the **MailboxType** column) the retention policy is assigned to.

How often will I see these service advisories?

If you don't take action to resolve the quota issues, you can expect to see this type of service advisory every seven days. Subsequent service advisories may contain higher mailbox counts for other mailboxes that are nearing their quota. If you take action to resolve quota issues, this service advisory will only occur when another mailbox with quota issues is identified.

More information

- For information about troubleshooting and resolving archive mailbox issues, see [Microsoft Purview troubleshooting](#).
- For guidance about identifying the holds placed on a mailbox, see [How to identify the type of hold placed on a mailbox](#).

Service advisories for eDiscovery throttling in Exchange Online monitoring

10/28/2022 • 2 minutes to read • [Edit Online](#)

We've released a new Exchange Online service advisory that informs you of eDiscovery being throttled. These service advisories provide visibility into the instances when the user is unable to submit Search and Export because of throttling.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to **Health | Service health | Exchange Online**. Here's an example of eDiscovery service advisory.

The screenshot shows the Microsoft 365 Service Health page. On the left, the 'Service health' section is active, showing a list of issues. The 'Active issues' section is expanded, showing a table of issues. The 'eDiscovery keyword searches and export jobs throttled in your tenant' issue is highlighted. On the right, a detailed view of this advisory is shown. It includes the title, ID (EX443330), last updated time (October 6, 2022 2:50 PM), and estimated start time (October 6, 2022 2:50 PM). The 'Affected services' section lists 'Exchange Online'. The 'Issue type' is 'Advisory' and the 'Issue origin' is 'Your environment'. The 'Status' is 'Investigating'. The 'User impact' section states that if action is not taken, eDiscovery keyword searches and export jobs may fail. The 'Action needed' section advises waiting for existing queries to complete and ensuring operations are within defined search limits. The 'Additional diagnostics' section provides a link to 'Limits for eDiscovery search | Microsoft Docs'. The 'All updates' section shows the advisory was updated on October 6, 2022 2:50 PM.

Issue title	Affected service	Issue type
Microsoft service health (7)		
Guest users without Microsoft Teams licenses can't utilize the chat within internally hosted Microsoft Teams meetings	Microsoft Teams	Advisory
Users migrated from Skype for Business to Microsoft Teams may be unable to unblock internal users	Microsoft Teams	Advisory
Admins may notice provisioning delays after performing Microsoft Teams data object or user changes	Microsoft Teams	Advisory
Admins are not seeing alerts generated in Microsoft Teams, OneDrive for Business, and SharePoint Online	Microsoft 365 suite, Microsoft Teams	Advisory
Some admins may not see up to date information for multiple usage reports in the Microsoft 365 admin center	Microsoft 365 suite	Advisory
Some users may be receiving spam email messages containing JCS attachments from Outlook.com addresses in their inbox	Exchange Online	Advisory
Users' outgoing email messages on Outlook on the web may be saved in the Drafts folder instead of the Sent folder	Exchange Online	Advisory
Issues in your environment that require action (2)		
Exchange Online Basic Auth Deprecation in Progress	Exchange Online	Advisory
eDiscovery keyword searches and export jobs throttled in your tenant	Exchange Online	Advisory

What does this service advisory indicate?

The service advisories for eDiscovery throttling inform admins about their tenant being throttled due to number of Search and Export jobs exceeding the limit set by Microsoft. Various limits are applied to eDiscovery search tools in the [Microsoft Purview](#) compliance portal. This includes searches run on the [Content Search](#) page and searches that are associated with an eDiscovery case on the [eDiscovery \(Standard\)](#) page. These limits help to maintain the health and quality of services provided to organizations. These advisories provide awareness so that you can take these limits into consideration when planning, running, and troubleshooting eDiscovery searches and exports.

For limits related to the Microsoft Purview eDiscovery (Standard) tool, see [Limits for Content search and eDiscovery \(Standard\) in the compliance center](#).

How often will I see these service advisories?

You can expect to see this type of advisory until the time where the Search and Export jobs are within the defined limit.

More information

- For information about troubleshooting and resolving eDiscovery compliance issues, see [Microsoft Purview](#)

[troubleshooting](#).

- For information about Microsoft Purview, see [What is Microsoft Purview?](#)
- To learn more about Microsoft Purview eDiscovery solutions, see [Microsoft Purview eDiscovery solutions](#)

Service advisories for MRS source delays in Exchange Online monitoring

10/28/2022 • 2 minutes to read • [Edit Online](#)

Mailbox Replication Service (MRS) source delay service advisories inform you of storage limitations or high processor utilization issues on the tenant side (migration source) that might be delaying mailbox migrations in your Microsoft 365 organization. These service advisories also include links to Microsoft resources to help you resolve these issues.

These service advisories are displayed in the Microsoft 365 admin center. To view these service advisories, go to **Health > Service health > Exchange Online** and then click the **Active issues** tab.

What do these service advisories indicate?

This service advisory informs you of potential delays to mailbox migrations in your organization. This includes cross-forest migrations, onboarding migrations, and offboarding migrations. The service advisory contains a table with information about the current migrations in your organization. Here's an example of the table with information about migration delays.

BATCHGUID	EXCHANGE GUID	REQUESTGUID	DELAYREASON	QUEUEDHOURS	DELAYINHOURS	SOURCESERVER	REMOVEDATABASENAME
12345678-1234-1234-1234-1234567891011	246c21f7-ca3c-4bba-ab5d-23456558c52a	3d7fab16-7d8e-4c81-a849-e0795054292a	DiskLatency	35.2	27.3	RD1GBL01EXCH003	GBL01EDAG001-db002
87654321-4321-4321-4321-1101987654321	21e9a608-78c3-44ef-a4dd-d5e7222aae82	9974aeb4-2aa4-4a2c-aeb6-d94d78cc25c9	DiskLatency	0.4	0.9	RD1GBL01EXCH010	GBL01EDAG010-db003

The following list describes each column in the previous example.

- **BatchGuid:** Unique GUID for the migration job.
- **ExchangeGuid:** The globally unique identifier (GUID) of the user mailbox that's being migrated.
- **RequestGuid:** The GUID of the migration request.
- **DelayReason:** The reason for the delayed migration.
- **QueueHours:** The duration the migration has been queued and waiting.
- **DelayInHours:** The duration the migration has been delayed.
- **SourceServer:** The on-premises server the migration originates from.
- **RemoteDatabaseName:** The database name the migration originates from.

More information

For more information about MRS and mailbox migrations, see the following articles:

- [Mailbox moves in Exchange](#)
- [Microsoft 365 and Office 365 migration performance and best practices](#)
- [Mailbox migration performance analysis](#)
- [Troubleshooting slow migrations](#)
- [Ways to migrate multiple email accounts to Microsoft 365](#)

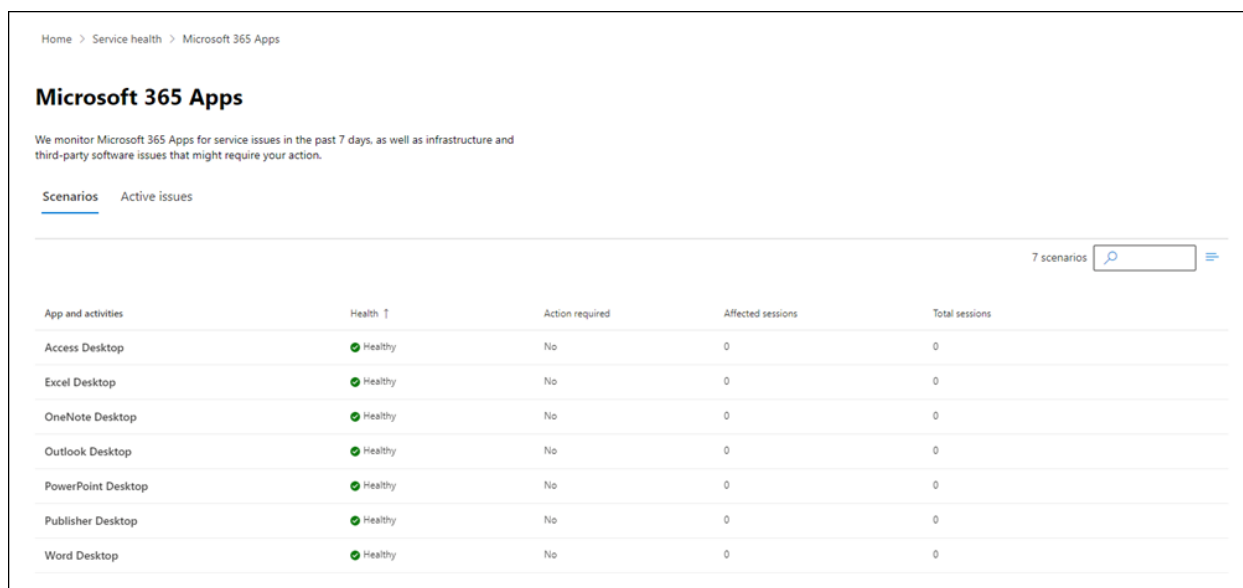
Microsoft 365 Apps monitoring

10/28/2022 • 2 minutes to read • [Edit Online](#)

Microsoft 365 Apps monitoring supports the following organizational-level scenarios for these desktop Office applications: Access, Excel, OneNote, Outlook, PowerPoint, Publisher, and Word.

- **Excessive Client Runtime Errors.** The runtime error rate of specific Office application has increased significantly over the last 24 hours.
- **Long Local File Load Time.** The average file load time from local storage has exceeded the recommended threshold over the last 24 hours.
- **Long Application Load Time.** The average application load time has exceeded the recommended threshold over the last 24 hours.
- **Excessive Macro Errors.** The macro error rate has exceeded the recommended threshold over the last 24 hours.
- **Excessive Add-in Errors.** The add-in error rate has exceeded the recommended threshold over the last 24 hours.
- **Long SharePoint File Load Time.** The average file load time from SharePoint has exceeded the recommended threshold over the last 24 hours.

Here's an example of the Apps monitoring dashboard



Home > Service health > Microsoft 365 Apps

Microsoft 365 Apps

We monitor Microsoft 365 Apps for service issues in the past 7 days, as well as infrastructure and third-party software issues that might require your action.

Scenarios Active issues

7 scenarios

App and activities	Health ↑	Action required	Affected sessions	Total sessions
Access Desktop	Healthy	No	0	0
Excel Desktop	Healthy	No	0	0
OneNote Desktop	Healthy	No	0	0
Outlook Desktop	Healthy	No	0	0
PowerPoint Desktop	Healthy	No	0	0
Publisher Desktop	Healthy	No	0	0
Word Desktop	Healthy	No	0	0

When Microsoft detects an error condition, a post is created to notify the tenant admin to go to the Microsoft 365 App Health dashboard for further information to remediate issues. For more information, see [Microsoft 365 Apps health](#).

Setup guides for Microsoft 365 and Office 365 services

10/28/2022 • 16 minutes to read • [Edit Online](#)

Microsoft 365 and Office 365 setup guides give you tailored guidance and resources for planning and deploying your tenant, apps, and services. These guides are created using the same best practices that [Microsoft 365 FastTrack](#) onboarding specialists share in individual interactions, and they're available to all admins within the Microsoft 365 admin center. They give information on product setup, enabling security features, deploying collaboration tools, and provide scripts to speed up advanced deployments.

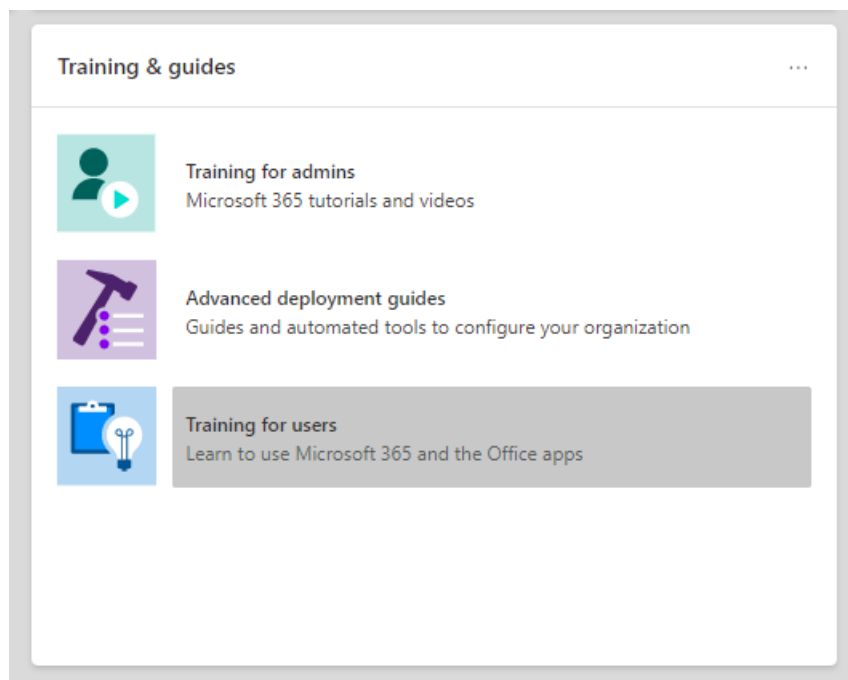
NOTE

You must be assigned an admin role like Global Reader to access the Microsoft 365 setup guides. Only admins with the Global Administrator role can use the guides to change settings in the tenant.

How to access setup guides in the Microsoft 365 admin center

The setup guides are accessible from the [Setup guidance](#) page in the Microsoft 365 admin center. You can keep track of the status of your progress and return at any time to complete a guide. To reach the **Setup guidance** page:

1. In the [Microsoft 365 admin center](#), go to the **Home** page.
2. Find the **Training & guides** card.



3. Select **Advanced deployment guides** and then select **All guides**.

Microsoft 365 admin center

Search

Home

Users

Active users

Contacts

Guest users

Deleted users

Devices

Teams & groups

Roles

Resources

Billing

Support

Settings

Setup

Reports

Health

Admin centers

Security

Compliance

Endpoint Manager

Azure Active Directo...

Home > Advanced deployment guides

Advanced deployment guides

Overview All guides Training resources Request assistance

Here are all guides sorted by category. Use the filter or search to find a specific guide to deploy services and features to your environment.

Completed0

In progress0

Not started40

Filters:

Category: All

Product: All

Status: All

Name	Services
Initial setup	
Prepare your environment	Office Exchange
Email setup guide	Exchange
Migrate Gmail contacts and calendar items	Exchange
Microsoft 365 setup guide	Windows 10

Guides for initial setup

Prepare your environment

The [Prepare your environment](#) guide helps you prepare your organization's environment for Microsoft 365 and Office 365 services. Whatever your goals are, there are tasks you'll need to complete to ensure a successful deployment. To avoid any errors while preparing your environment, you're provided with step-by-step instructions to connect your domain, add users, assign licenses, set up email with Exchange Online, and install or deploy Office apps.

Email setup guide

The [Email setup guide](#) provides you with the step-by-step guidance needed for configuring Exchange Online for your organization. This guidance includes setting up new email accounts, migrating email, and configuring email protection. For a successful email setup, use this advisor and you'll receive the recommended migration method based on your organization's current mail system, the number of mailboxes being migrated, and how you want to manage users and their access.

Migrate Gmail contacts and calendar items

When you migrate a Gmail user's mailbox to Microsoft 365, email messages are migrated, but contacts and calendar items are not. The [Gmail contacts and calendar advisor](#) provides steps for importing Google contacts and Google calendar items to Microsoft 365 using import and export methods with Outlook.com, the Outlook client, or PowerShell.

Microsoft 365 setup guide

The [Microsoft 365 setup guide](#) provides you with guidance when setting up productivity tools, security policies, and device management capabilities. With a Microsoft 365 Business Premium or Microsoft 365 for enterprise subscription, you can use this advisor to set up and configure your organization's devices.

You'll receive guidance and access to resources to enable your cloud services, update devices to the latest supported version of Windows 10, and join devices to Azure Active Directory (Azure AD), all in one central location.

Remote work setup guide

The [Remote work setup guide](#) provides organizations with the tips and resources needed to ensure your users can successfully work remotely, your data is secure, and users' credentials are safeguarded.

You'll receive guidance to optimize remote workers' device traffic to both Microsoft 365 resources in the cloud and your organization's network, which will reduce the strain on your remote access VPN infrastructure.

Microsoft Edge setup guide

Microsoft Edge has been rebuilt from the ground up to bring you world-class compatibility and performance, the security and privacy you deserve, and new features designed to bring you the best of the web.

The [Microsoft Edge setup guide](#) will help you configure Enterprise Site Discovery to see which sites accessed in your org might need to use IE mode, review and configure important security features, configure privacy policies and compliance policies to meet your org's requirements, and manage web access on your devices. You can download Microsoft Edge to individual devices, or we'll show you how to deploy to multiple users in your org with Group Policy, Configuration Manager, or Microsoft Intune.

Configure IE mode for Microsoft Edge

If you've already deployed Microsoft Edge and only want to configure IE mode, the [Configure IE mode for Microsoft Edge guide](#) will give you scripts to automate the configuration of Enterprise Site Discovery. You'll also get IE mode recommendations from a cloud-based tool that will help you create an Enterprise Mode Site List to deploy to your users.

Microsoft Search setup guide

Microsoft Search helps your organization find what they need to complete what they're working on. Whether it's searching for people, files, org charts, sites, or answers to common questions, your org can use Microsoft Search throughout their workday to get answers.

The [Microsoft Search setup guide](#) helps you configure Microsoft Search whether you want to pilot it to a group of users or roll it out to everyone in your org. You'll assign Search admins and Search editors and then customize the search experience for your users with answers and more options, like adding the Bing extension to Chrome or setting Bing as your default search engine.

Block use of Internet Explorer in your organization

Microsoft support for Internet Explorer 11 is ending soon for most versions of Windows 10. The [Block use of Internet Explorer in your organization guide](#) ensures that your users can still run legacy web apps that rely on Internet Explorer. This guide also helps you move those users to Microsoft Edge with IE mode.

Guides for authentication and access

Configure multi-factor authentication (MFA)

The [Configure multi-factor authentication \(MFA\) guide](#) provides information to secure your organization against breaches due to lost or stolen credentials. MFA immediately increases account security by prompting for multiple forms of verification to prove a user's identity when they sign in to an app or other company resource. This prompt could be to enter a code on the user's mobile device or to provide a fingerprint scan. MFA is enabled through Conditional Access, security defaults, or per-user MFA. This guide will provide the recommended MFA option for your org, based on your licenses and existing configuration.

Identity security for Teams

The [Identity security for teams guide](#) helps you with some basic security steps you can take to ensure your users are safe and have the most productive time using Teams.

Add or sync users to Microsoft 365

[This guide](#) will help streamline the process of getting your user accounts set up in **Microsoft 365**. Based on your environment and needs, you can choose to add users individually, migrate your on-premises directory with Azure AD cloud sync or Azure AD Connect, or troubleshoot existing sync problems when necessary.

Azure AD setup guide

The [Azure AD setup guide](#) provides information to ensure your organization has a strong security foundation. In this guide you'll set up initial features, like Azure Role-based access control (Azure RBAC) for admins, Azure AD Connect for your on-premises directory, and Azure AD Connect Health, so you can monitor your hybrid identity's health during automated syncs.

It also includes essential information on enabling self-service password resets, conditional access and integrated third party sign-on including optional advanced identity protection and user provisioning automation.

Sync users from your Windows Server Active Directory

The [Sync users from your Windows Server Active Directory](#) guide walks you through turning on directory synchronization. Directory synchronization brings your on-premises and cloud identities together for easier access and simplified management. Unlock new capabilities, like single sign-on, self-service options, automatic account provisioning, conditional access controls, and compliance policies. These capabilities ensure your users have access to the resources they need from anywhere.

Plan your passwordless deployment

Upgrade to an alternative sign-in approach that allows users to access their devices securely with one of the following passwordless authentication methods:

- Windows Hello for Business
- The Microsoft Authenticator app
- Security keys

Use the [Plan your passwordless deployment](#) guide to discover the best passwordless authentication methods to use and receive guidance on how to deploy them.

Integrate a third-party cloud app with Azure AD

[This guide](#) helps IT admins to select and configure the App.

Plan your self-service password reset (SSPR) deployment

Give users the ability to change or reset their password independently, if their account is locked, or they forget their password without the need to contact a helpdesk engineer.

Use the [Plan your self-service password reset deployment](#) guide to receive relevant articles and instructions for configuring the appropriate Azure portal options to help you deploy SSPR in your environment.

Guides for security and compliance

Security analyzer

The [Security analyzer](#) will analyze your security approach and introduce you to Microsoft integrated security and compliance solutions that can improve your security posture. You'll learn about advanced features, such as managing identities and helping to protect against modern attacks. You can then sign up for a trial subscription and be pointed to the corresponding setup guidance for each solution.

Microsoft Intune setup guide

Set up Microsoft Intune to manage devices in your organization. For full control of corporate devices, you'll use Intune's mobile device management (MDM) features. To manage your organization's data on shared and personal devices, you can use Intune's mobile application management (MAM) features.

With the [Microsoft Intune setup guide](#), you'll set up device and app compliance policies, assign app protection policies, and monitor the device and app protection status.

Microsoft Defender for Endpoint setup guide

The [Microsoft Defender for Endpoint setup guide](#) provides instructions that will help your enterprise network prevent, detect, investigate, and respond to advanced threats. Make an informed assessment of your organization's vulnerability and decide which deployment package and configuration methods are best.

NOTE

A Microsoft Volume License is required for Microsoft Defender for Endpoint.

Exchange Online Protection setup guide

Microsoft Exchange Online Protection (EOP) is a cloud-based email filtering service for protection against spam and malware, with features to safeguard your organization from messaging policy violations.

Use the [Exchange Online Protection setup guide](#) to set up EOP by selecting which of the three deployment scenarios—on-premises mailboxes, hybrid (mix of on-premises and cloud) mailboxes, or all cloud mailboxes—fits your organization. The guide provides information and resources to set up and review your user's licensing, assign permissions in the Microsoft 365 admin center, and configure your organization's anti-malware and spam policies in the Security & Compliance Center.

Microsoft Defender for Office 365 setup guide

The [Microsoft Defender for Office 365 setup guide](#) safeguards your organization against malicious threats that your environment might come across through email messages, links, and third party collaboration tools. This guide provides you with the resources and information to help you prepare and identify the Defender for Office 365 plan to fit your organization's needs.

Microsoft Defender for Identity setup guide

The [Microsoft Defender for Identity setup guide](#) provides security solution set-up guidance to identify, detect, and investigate advanced threats that might compromise user identities. These include detecting suspicious user activities and malicious insider actions directed at your organization. You'll create a Defender for Identity instance, connect to your organization's Active Directory, and then set up sensors, alerts, notifications, and configure your unique portal preferences.

Insider risk solutions setup guide

The [Insider risk solutions setup guide](#) helps you protect your organization against insider risks that can be challenging to identify and difficult to mitigate. Insider risks occur in a variety of areas and can cause major problems for organizations, ranging from the loss of intellectual property to workplace harassment, and more.

The solutions in this guide will help you gain visibility into user activities, actions, and communications with native signals and enrichments from across your organization:

- With the communication compliance solution, you can identify and act on communication risks for items like workplace violence, insider trading, harassment, code of conduct, and regulatory compliance violations.
- The insider risk management solution helps you identify, investigate, and take action on risks for intellectual property theft, sensitive data leaks, security violations, data spillage, and confidentiality violations.

Microsoft Purview Information Protection setup guide

Get an overview of the capabilities you can apply to your information protection strategy so you can be confident your sensitive information is protected. Use a four-stage lifecycle approach in which you discover, classify, protect, and monitor sensitive information. The [Microsoft Purview Information Protection setup guide](#) provides guidance for completing each of these stages.

Microsoft Purview Data Lifecycle Management setup guide

The [Microsoft Purview Data Lifecycle Management setup guide](#) provides you with the information you'll need to set up and manage your organization's governance strategy, to ensure that your data is classified and managed according to the specific lifecycle guidelines you set. With this guide, you'll learn how to create, auto-apply, or publish retention labels, retention label policies, and retention policies that are applied to your organization's content and compliance records. You'll also get information on importing CSV files with a file plan for bulk scenarios or for applying them manually to individual documents.

Microsoft Defender for Cloud Apps setup guide

The [Microsoft Defender for Cloud Apps setup guide](#) provides easy to follow deployment and management guidance to set up your Cloud Discovery solution. With Cloud Discovery, you'll integrate your supported security apps, and then you'll use traffic logs to dynamically discover and analyze the cloud apps that your organization uses. You'll also set up features available through the Defender for Cloud Apps solution, including threat detection policies to identify high-risk use, information protection policies to define access, and real-time session controls to monitor activity. With these features, your environment gets enhanced visibility, control over data movement, and analytics to identify and combat cyberthreats across all your Microsoft and third party cloud services.

Audit solutions setup guide

The [Microsoft 365 auditing solutions guide](#) provides an integrated solution to help organizations effectively respond to security events, forensic investigations, and compliance obligations. When you use the auditing solutions in Microsoft 365, you can search the audit log for activities performed in different Microsoft 365 services.

eDiscovery solutions setup guide

eDiscovery is the process of identifying and delivering electronic information that can be used as evidence in legal cases. The eDiscovery solutions setup guide assists in the use of eDiscovery tools in Microsoft Purview that allow you to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer communities.

Guides for collaboration

Build your employee experience

Transform how your employees work together with the [Employee experience dashboard](#). For seamless teamwork, use Microsoft 365 to create productive, aligned teams, and keep employees engaged with leadership and the rest of the organization. Help your employees be effective in all work activities. These guides will provide instructions on how to use SharePoint, Teams, and Yammer to build collaboration across your org to help drive productivity.

Microsoft 365 Apps setup guide

The [Microsoft 365 Apps setup guide](#) helps you get your users' devices running the latest version of Office products like Word, Excel, PowerPoint, and OneNote. You'll get guidance on the various deployment methods that include easy self-install options to enterprise deployments with management tools. The instructions will help you assess your environment, figure out your specific deployment requirements, and implement the necessary support tools to ensure a successful installation.

Mobile apps setup guide

The [Mobile apps setup guide](#) provides instructions for the download and installation of Office apps on your Windows, iOS, and Android mobile devices. This guide provides you with step-by-step information to download and install Microsoft 365 and Office 365 apps on your phone and tablet devices.

Microsoft Teams setup guide

The [Microsoft Teams setup guide](#) provides your organization with guidance to set up team workspaces that host

real-time conversations through messaging, calls, and audio or video meetings for both team and private communication. Use the tools in this guide to configure Guest access, set who can create teams, and add team members from a .csv file, all without the need to open a PowerShell session. You'll also get best practices for determining your organization's network requirements and ensuring a successful Teams deployment.

Teams Phone setup guide

The [Teams Phone setup guide](#) helps you stay connected with the use of modern calling solutions. Apply key capabilities with a cloud-based, call-control system that supports the telephony workload for Teams. You can choose and deploy features from the available public switched telephone network (PSTN) connectivity options. You can also find assistance for other features, such as auto attendant, call queues, Audio Conferencing, caller ID, and live events.

SharePoint setup guide

The [SharePoint setup guide](#) helps you set up your SharePoint document storage and content management, create sites, configure external sharing, migrate data and configure advanced settings, and drive user engagement and communication within your organization. You'll follow steps for configuring your content-sharing permission policies, choose your migration sync tools, and enable the security settings for your SharePoint environment.

OneDrive setup guide

Use the [OneDrive setup guide](#) to get started with OneDrive file storage, sharing, collaboration, and syncing capabilities. OneDrive provides a central location where users can sync their Microsoft 365 Apps files, configure external sharing, migrate user data, and configure advanced security and device access settings. The OneDrive setup guide can be deployed using a OneDrive subscription or a standalone OneDrive plan.

Yammer deployment advisor

Connect and engage across your organization with Yammer. The [Yammer deployment advisor](#) prepares your Yammer network by adding domains, defining admins, and combining Yammer networks. You'll get guidance to deploy Yammer and then customize the look, configure security and compliance, and refine the settings.

Advanced guides

In-place upgrade with Configuration Manager

Use the [In-place upgrade with Configuration Manager guide](#) when upgrading Windows 7 and Windows 8.1 devices to the latest version of Windows 10. You'll use the script provided to check the prerequisites and automatically configure an in-place upgrade.

Deploy Office to your users

Deploy Office apps from the cloud with the ability to customize your installation by using the Office Deployment Tool. The [Deploy Office to your users guide](#) helps you create a customized Office configuration with advanced settings, or you can use a pre-built recommended configuration. Whether your users are conducting a self-install or you're deploying to your users individually or in bulk, this advanced guide provides you with step-by-step instructions to give users an Office installation tailored to your organization.

Deploy Office to remote users

Now that working remotely is the norm, users need to receive your organization's Office settings when they're not connected to your internal network or when using their own devices.

Use the [Deploy Office to remote users guide](#) to create a customized Office installation and then send users a generated PowerShell script that will seamlessly install Office with your configuration.

Deploy and update Microsoft 365 Apps with Configuration Manager

For organizations using Configuration Manager, you can use the [Deploy and update Microsoft 365 Apps with Configuration Manager advisor](#) to generate a script that will automatically configure your Microsoft 365 Apps

deployment using best practices recommended by FastTrack engineers. Use this guide to build your deployment groups, customize your Office apps and features, configure dynamic or lean installations, and then run the script to create the applications, automatic deployment rules, and device collections you need to target your deployment.

Intune Configuration Manager co-management setup guide

Use the [Intune Configuration Manager co-management setup guide](#) to set up existing Configuration Manager client devices and new internet-based devices that your org wants to co-manage with both Microsoft Intune and Configuration Manager. Co-management allows you to manage Windows 10 devices and adds new functionality to your org's devices, while receiving the benefits of both solutions.

School Data Sync rollover setup guide

The [SDS Rollover setup guide](#) provides the steps to help your organization sync student information data to Azure Active Directory and Office 365. This guide streamlines the term lifecycle management process by creating Office 365 Groups for Exchange Online and SharePoint Online, class teams for Microsoft Teams and OneNote, as well as Intune for Education, and rostering and single sign-on integration for third-party apps. You'll perform end-of-year closeout, tenant cleanup and archive, new school year preparation, and new school year launch. Then you can create new profiles using the sync deployment method that suits your organization.

Microsoft 365 inter-tenant collaboration

10/28/2022 • 6 minutes to read • [Edit Online](#)

Suppose that two organizations, Fabrikam and Contoso, each have a Microsoft 365 for business tenant and they want to work together on several projects; some of which run for a limited time and some of which are ongoing. How can Fabrikam and Contoso enable their people and teams to collaborate more effectively across their different Microsoft 365 tenants in a secure manner? Microsoft 365, in conjunction with Azure Active Directory (Azure AD) B2B collaboration, provides several options. This article describes several key scenarios that Fabrikam and Contoso can consider.

Microsoft 365 inter-tenant collaboration options include using a central location for files and conversations, sharing calendars, using IM, audio/video calls for communication, and securing access to resources and applications. Use the following tables to select solutions and learn more.

Exchange Online collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Share calendars with another Microsoft 365 organization	Administrators can set up different levels of calendar access in Exchange Online to allow businesses to collaborate with other businesses and to let users share the schedules (free/busy information) with others.	• Sharing • Organization relationships • Create an organization relationship • Modify an organization relationship • Remove an organization relationship • Share calendars with external users
Control how users share their calendars with people outside your organization	Administrators apply sharing policies to users mailboxes to control who it can be shared with and the level of access granted	• Sharing policies • Create a sharing policy • Apply a sharing policy to mailboxes • Modify, disable, or remove a sharing policy
Configure secure email channels and control mail flow with partner organizations	Administrators create connectors to apply security to mail exchanges with a partner organization or service provider. The connectors enforce encryption via transport layer security (TLS) as well as allowing restrictions on domain names or IP address ranges your partners send email from.	• How Exchange Online uses TLS to secure email connections • Configure mail flow using connectors • Remote domains • Set up connector for secure mail flow with a partner organization • Mail flow best practices (overview)

SharePoint Online and OneDrive for Business collaboration options

SHARING GOALS	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Share sites and documents with external users	Administrators configure sharing at the tenant, or site collection level for Microsoft account authenticated, work or school account authenticated or guest accounts	• Manage external sharing for your SharePoint Online environment • Restrict sharing of SharePoint and OneDrive content by domain • Use SharePoint Online as a business-to-business (B2B) extranet solution
Tracking and controlling external sharing for end users	OneDrive for Business file owners and SharePoint Online end users configure site and document sharing and establish notifications to track sharing	• Configure notifications for external sharing for OneDrive for Business • Share SharePoint files or folders

Skype for Business collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Skype for Business Online - IM, calls, and presence with other Skype for Business users	Administrators can enable their Skype for Business Online users to IM, make audio/video calls, and see presence with users in another Microsoft 365 tenant.	Allow users to contact external Skype for Business users
Skype for Business Online - IM, calls, and presence with Skype (consumer) users	Administrators can enable their Skype for Business Online users to IM, make calls, and see presence with Skype (consumer) users.	Let Skype for Business users add Skype contacts

Azure AD B2B Collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Azure AD B2B collaboration - Content sharing by adding external users to a group in an organization's directory	A Azure AD DC admin, Security Admin, User Admin, Cloud Application Admin, or Global admin for one Microsoft 365 tenant can invite people in another Microsoft 365 tenant to join their directory, add those external users to a group, and grant access to content, such as SharePoint sites and libraries for the group.	• What is Azure AD B2B collaboration preview? • Azure AD B2B: New updates make cross-business collab easy • External sharing and Azure Active Directory B2B collaboration • Azure Active Directory B2B collaboration API and customization • Azure AD and Identity Show: Azure AD B2B Collaboration (Business to Business)

Microsoft 365 collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Microsoft 365 Groups - Email, calendar, OneNote, and shared files in a central place	Groups are supported in Business Essentials, Business Premium, Education, and the Enterprise E1, E3, and E5 plans. People in one Microsoft 365 tenant can create a group and invite people in another Microsoft 365 tenant as guest users. Applies to Dynamics CRM as well.	• Learn about Microsoft 365 groups • Guest access in Microsoft 365 Groups • Deploy Microsoft 365 Groups

Yammer collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Yammer - Collaboration through an enterprise social medium	Unless the ability to create external groups is disabled by a Yammer admin, users can create external groups to collaborate in Yammer through conversations, the ability to like and follow posts, share files, and chat online.	Create and manage external groups in Yammer

Teams collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Collaborate in Teams with users external to the organization	A User Admin , or Global admin for the inviting Microsoft 365 tenant needs to enable external collaboration in Teams. Global admins and team owners will now be able to invite anyone with an email address to collaborate in Teams. Admins can also manage and edit Guests already present in their tenant.	• Authorize Guest Access • Turn Guest Access On or Off in Teams • Use PowerShell to control Guest Access • Guest Access Checklist • View Guest Users • Edit guest user information
Team owners can invite and manage how guests collaborate within their teams.	Team owners have additional controls on what the guests can do within their teams.	• Add Guests • Add a guest to a team • Manage Guest Access in Teams • See who's on a Team or in a Channel
Guests from other tenants can view contents in Teams and collaborate with other members	None.	The guest access experience

Power BI collaboration options

SHARING GOAL	ADMINISTRATIVE ACTION	HOW-TO INFORMATION
Power BI enables external guest users to consume content shared to them through links. This enables users in the organization to distribute content in a secure way across organizations.	The Power BI Admin can control whether users can invite external users to view content within the organization.	Distribute Power BI content to external guest users with Azure AD B2B

Points to be aware of about Microsoft 365 inter-tenant collaboration

Sharing of user accounts, licenses, subscriptions, and storage

Each organization maintains its own user accounts, identities, security groups, subscriptions, licenses, and storage. People use the collaboration features in Microsoft 365 together with sharing policies and security settings to provide access to needed information while maintaining control of company assets.

- **User accounts:** Accounts cannot be shared or duplicated between the tenants or partitions in the on-premises Active Directory Domain Services.
- **Licenses & subscriptions:** In Microsoft 365, licenses from licensing plans (also called SKUs or Microsoft 365 plans) give users access to the Microsoft 365 services that are defined for those plans.
- **Storage:** In Microsoft 365 licensing plans, software boundaries and limits for SharePoint Online are managed separately from mailbox storage limits. Mailbox storage limits are set up and managed by using Exchange Online. In both scenarios, storage can't be shared across tenants.

Can we share domain namespaces across Microsoft 365 tenants?

No. Organization domain names, such as fabrikam.com or tailspintoys.com, can only be associated and used with a single Microsoft 365 tenant. Each tenant must have its own namespace. UPN, SMTP, and SIP namespaces cannot be shared across tenants.

What about hybrid components and Microsoft 365 inter-tenant collaboration?

On-premises hybrid components, such as an Exchange organization and Azure AD Connect, cannot be split across multiple tenants.

Cross-tenant mailbox migration (preview)

10/28/2022 • 30 minutes to read • [Edit Online](#)

Commonly, during mergers or divestitures, you need the ability to move your users' Exchange Online mailboxes into a new tenant. Cross-tenant mailbox migration allows tenant administrators to use well-known interfaces like Exchange Online PowerShell and MRS to transition users to their new organization.

Administrators can use the **New-MigrationBatch** cmdlet, available through the *Move Mailboxes* management role, to execute cross-tenant moves.

Users migrating must be present in the target tenant Exchange Online system as MailUsers, marked with specific attributes to enable the cross-tenant moves. The system will fail moves for users that aren't properly set up in the target tenant.

When the moves are complete, the source user mailbox is converted to a MailUser and the targetAddress (shown as ExternalEmailAddress in Exchange) is stamped with the routing address to the destination tenant. This process leaves the legacy MailUser in the source tenant and allows for coexistence and mail routing. When business processes allow, the source tenant may remove the source MailUser or convert them to a mail contact.

Cross-tenant Exchange mailbox migrations are supported for tenants in hybrid or cloud only, or any combination of the two.

This article describes the process for cross-tenant mailbox moves and provides guidance on how to prepare source and target tenants for the Exchange Online mailbox content moves.

IMPORTANT

Do not use this feature to migrate mailboxes on any type of hold. Migrating source mailboxes for users on hold is not supported.

When a mailbox is migrated cross-tenant with this feature, only user visible content in the mailbox (email, contacts, calendar, tasks, and notes) is migrated. to the target (destination tenant). After successful migration, the source mailbox is deleted. This means that after the migration, under no circumstances, is the source mailbox available, discoverable, or accessible in the source tenant.

NOTE

If you are interested in previewing our new feature Domain Sharing for email alongside your cross-tenant mailbox migrations, please complete the form at aka.ms/domainsharingpreview. Domain sharing for email enables users in separate Microsoft 365 tenants to send and receive email using addresses from the same custom domain. The feature is intended to solve scenarios where users in separate tenants need to represent a common corporate brand in their email addresses. The current preview supports sharing domains indefinitely and shared domains during cross-tenant mailbox migration coexistence.

Preparing source and target tenants

Prerequisites for source and target tenants

Before starting, be sure you have the necessary permissions to configure the Move Mailbox application in Azure, EXO Migration Endpoint, and the EXO Organization Relationship.

Additionally, at least one mail-enabled security group in the source tenant is required. These groups are used to scope the list of mailboxes that can move from source (or sometimes referred to as resource) tenant to the

target tenant. This allows the source tenant admin to restrict or scope the specific set of mailboxes that need to be moved, preventing unintended users from being migrated. Nested groups aren't supported.

You'll also need to communicate with your trusted partner company (with whom you will be moving mailboxes) to obtain their Microsoft 365 tenant ID. This tenant ID is used in the Organization Relationship DomainName field.

To obtain the tenant ID of a subscription, sign in to the [Microsoft 365 admin center](#) and go to https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Properties. Click the copy icon for the Tenant ID property to copy it to the clipboard.

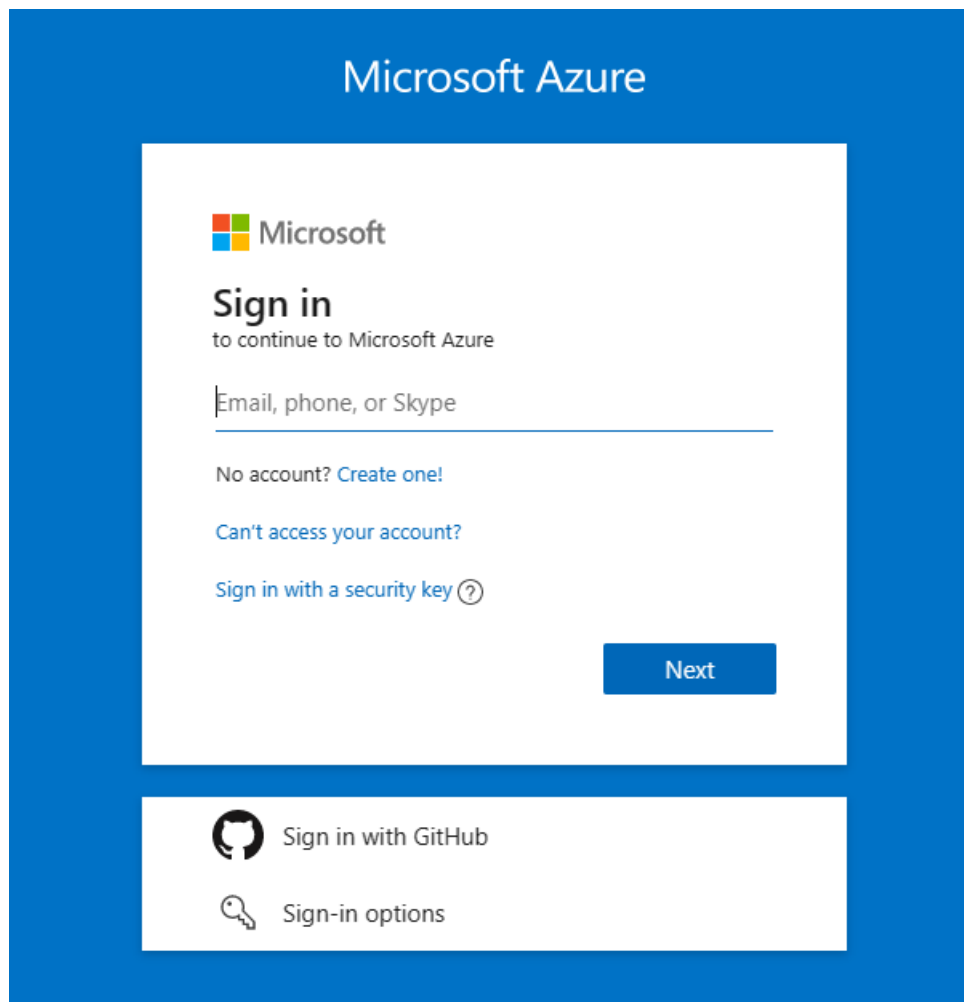
Configuration steps to enable your tenants for cross-tenant mailbox migrations

NOTE

You must configure the target (destination) first. To complete these steps, you are not required to have or know the tenant admin credentials for both source and target tenant. Steps can be performed individually for each tenant by different administrators.

Prepare the target (destination) tenant by creating the migration application and secret

1. Log in to your Azure AD portal (<https://portal.azure.com>) with your target tenant admin credentials



2. Click view under Manage Azure Active Directory.

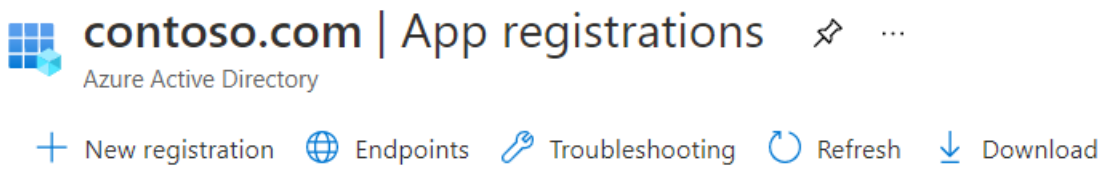


Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#)[Learn more](#)

3. On the left navigation bar, select App registrations.
4. Select New registration



5. On the Register an application page, under Supported account types, select Accounts in any organizational directory (Any Azure AD directory - Multitenant). Then, under Redirect URI (optional), select Web and enter <https://office.com>. Lastly, select Register.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

 ✓

Supported account types

Who can use this application or access this API?

- ☐ Accounts in this organizational directory only (test_test_msftofetesttenant-AdvancedEncryption only - Single tenant)
- ☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

6. On the top-right corner of the page, you'll see a notification pop-up that states the app was successfully created.

7. Go back to Home, Azure Active Directory and click on App registrations.
8. Under Owned applications, find the app you created and click on it.
9. Under ^Essentials, you'll need to copy down the Application (client) ID as you'll need it later to create a URL for the target tenant.
10. Now, on the left navigation bar, click on API permissions to view permissions assigned to your app.
11. By default, User. Read permissions are assigned to the app you created, but we don't require them for mailbox migrations, you can remove that permission.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for test_test_msftofetesttenant-AdvancedEncryption](#)

API / Permissions name	Type	Description	Admin consent requ...	Status	
▼ Microsoft Graph (1)					
User.Read	Delegated	Sign in and read user profile	No		...
					Remove permission

12. Now we need to add permission for mailbox migration, select Add a permission
13. In the Request API permissions windows, select APIs my organization uses, search for Office 365 Exchange Online, and select it.

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

office 365 exchange online
Name
Office 365 Exchange Online

14. Next, select Application permissions
15. Then, under Select permissions, expand Mailbox, check Mailbox.Migration, and Add permissions at the bottom on the screen.

Request API permissions



[← All APIs](#)



Office 365 Exchange Online

<https://ps.outlook.com>

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission	Admin consent required
> Other permissions	
> Calendars	
> Contacts	
> Exchange	
✓ Mailbox (1)	
☒ Mailbox.Migration ⓘ Move mailboxes between organizations	Yes
> MailboxSettings	
> Mail	

Add permissionsDiscard

16. Now select Certificates & secrets on the left navigation bar for your application.

17. Under Client secrets, select new client secret.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

18. In the Add a client secret window, enter a description, and configure your desired expiration settings.

NOTE

This is the password that will be used when creating your migration endpoint. It is extremely important that you copy this password to your clipboard and or copy this password to secure/secret password safe location. This is the only time you will be able to see this password! If you do somehow lose it or need to reset it, you can log back into our Azure portal, go to App registrations, find your migration app, select Secrets & certificates, and create a new secret for your app.

19. Now that you've successfully created the migration application and secret, you'll need to consent to the

application. To consent to the application, go back to the Azure Active Directory landing page, click on Enterprise applications in the left navigation, find your migration app you created, select it, and select Permissions on the left navigation.

20. Click on the Grant admin consent for [your tenant] button.
21. A new browser window will open and select Accept.
22. You can go back to your portal window and select Refresh to confirm your acceptance.
23. Formulate the URL to send to your trusted partner (source tenant admin) so they can also accept the application to enable mailbox migration. Here's an example of the URL to provide to them you'll need the application ID of the app you created:

```
https://login.microsoftonline.com/sourcetenant.onmicrosoft.com/adminconsent?client_id=[application_id_of_the_app_you_just_created]&redirect_uri=https://office.com
```

NOTE

You will need the application ID of the mailbox migration app you just created.

You will need to replace sourcetenant.onmicrosoft.com in the above example with your source tenants correct onmicrosoft.com name.

You will also need to replace [application_id_of_the_app_you_just_created] with the application ID of the mailbox migration app you just created.

Prepare the target tenant by creating the Exchange Online migration endpoint and organization relationship

1. [Connect to Exchange Online PowerShell](#) in the target Exchange Online tenant.
2. Create a new migration endpoint for cross-tenant mailbox moves

NOTE

You will need the application ID of the mailbox migration app you just created and the password (the secret) you configured during this process. Also depending on the Microsoft 365 Cloud Instance you use your endpoint may be different. Please refer to the [Microsoft 365 endpoints](#) page and select the correct instance for your tenant and review the Exchange Online Optimize Required address and replace as appropriate.

```
# Enable customization if tenant is dehydrated
$dehydrated=Get-OrganizationConfig | select isdehydrated
if ($dehydrated.isdehydrated -eq $true) {Enable-OrganizationCustomization}
$AppId = "[guid copied from the migrations app]"
$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $AppId,
(ConvertTo-SecureString -String "[this is your secret password you saved in the previous steps]" -
AsPlainText -Force)
New-MigrationEndpoint -RemoteServer outlook.office.com -RemoteTenant "sourcetenant.onmicrosoft.com" -
Credentials $Credential -ExchangeRemoteMove:$true -Name "[the name of your migration endpoint]" -
ApplicationId $AppId
```

3. Create new or edit your existing organization relationship object to your source tenant.

```

$sourceTenantId="[tenant id of your trusted partner, where the source mailboxes are]"
$orgrels=Get-OrganizationRelationship
$existingOrgRel = $orgrels | ?{$_ .DomainNames -like $sourceTenantId}
If ($null -ne $existingOrgRel)
{
    Set-OrganizationRelationship $existingOrgRel.Name -Enabled:$true -MailboxMoveEnabled:$true -
MailboxMoveCapability Inbound
}
If ($null -eq $existingOrgRel)
{
    New-OrganizationRelationship "[name of the new organization relationship]" -Enabled:$true -
MailboxMoveEnabled:$true -MailboxMoveCapability Inbound -DomainNames $sourceTenantId
}

```

Prepare the source (current mailbox location) tenant by accepting the migration application and configuring the organization relationship

1. From a browser, go to the URL link provided by your trusted partner to consent to the mailbox migration application. The URL will look like this:

```

https://login.microsoftonline.com/sourcetenant.onmicrosoft.com/adminconsent?client_id=
[application_id_of_the_app_you_just_created]&redirect_uri=https://office.com

```

NOTE

You will need the application ID of the mailbox migration app you just created. You will need to replace sourcetenant.onmicrosoft.com in the above example with your source tenants correct onmicrosoft.com name. You will also need to replace [application_id_of_the_app_you_just_created] with the application ID of the mailbox migration app you just created.

2. Accept the application when the pop-up appears. You can also log into your Azure Active Directory portal and find the application under Enterprise applications.
3. [Connect to Exchange Online PowerShell](#) on the source Exchange Online tenant.
4. Create a new organization relationship or edit your existing organization relationship object to your target (destination) tenant in Exchange Online PowerShell:

```

$targetTenantId="[tenant id of your trusted partner, where the mailboxes are being moved to]"
$appId="[application id of the mailbox migration app you consented to]"
$scope="[name of the mail enabled security group that contains the list of users who are allowed to migrate]"
$orgrels=Get-OrganizationRelationship
$existingOrgRel = $orgrels | ?{$_ .DomainNames -like $targetTenantId}
If ($null -ne $existingOrgRel)
{
    Set-OrganizationRelationship $existingOrgRel.Name -Enabled:$true -MailboxMoveEnabled:$true -
MailboxMoveCapability RemoteOutbound -OAuthApplicationId $appId -MailboxMovePublishedScopes $scope
}
If ($null -eq $existingOrgRel)
{
    New-OrganizationRelationship "[name of your organization relationship]" -Enabled:$true -
MailboxMoveEnabled:$true -MailboxMoveCapability RemoteOutbound -DomainNames $targetTenantId -
OAuthApplicationId $appId -MailboxMovePublishedScopes $scope
}

```

NOTE

The tenant ID that you enter as the \$sourceTenantId and \$targetTenantId is the GUID and not the tenant domain name. For an example of a tenant ID and information about finding your tenant ID, see [Find your Microsoft 365 tenant ID](#).

How do I know this worked?

You can verify cross-tenant mailbox migration configuration by running the [Test-MigrationServerAvailability](#) cmdlet against the cross-tenant migration endpoint that you created on your target tenant.

```
Test-MigrationServerAvailability -EndPoint "Migration endpoint for cross-tenant mailbox moves" -TestMailbox "Primary SMTP of MailUser object in target tenant"
```

Move mailboxes back to the original source

If a mailbox is required to move back to the original source tenant, the same set of steps and scripts will need to be run in both new source and new target tenants. The existing Organization Relationship object will be updated or appended, not recreated

Prepare target user objects for migration

Users migrating must be present in the target tenant and Exchange Online system (as MailUsers) marked with specific attributes to enable the cross-tenant moves. The system will fail moves for users that aren't properly set up in the target tenant. The following section details the MailUser object requirements for the target tenant.

Prerequisites for target user objects

Ensure the following objects and attributes are set in the target organization.

TIP

Microsoft is developing a feature to provide a secure automated method to set many of the attributes in the following section. This feature, named Cross-Tenant Identity Mapping, is currently looking for customers willing to participate in a small private preview. For more information about this pre-release feature and how it can simplify your cross-tenant migration processes, see the article [Cross-Tenant Identity Mapping](#).

1. For any mailbox moving from a source organization, you must provision a MailUser object in the Target organization:
 - The Target MailUser must have these attributes from the source mailbox or assigned with the new User object:
 - ExchangeGUID (direct flow from source to target): The mailbox GUID must match. The move process will not proceed if this isn't present on target object.
 - ArchiveGUID (direct flow from source to target): The archive GUID must match. The move process won't proceed if this isn't present on the target object. (This is only required if the source mailbox is Archive enabled).
 - LegacyExchangeDN (flow as proxyAddress, "x500:<LegacyExchangeDN>"): The LegacyExchangeDN must be present on target MailUser as x500: proxyAddress. In addition, you also need to copy all x500 addresses from the source mailbox to the target mail user. The move processes won't proceed if these aren't present on the target object. Also, this step is important for enabling reply ability for emails that are sent before migration. The sender/recipient address in each email item and the auto-complete cache in Microsoft Outlook and in Microsoft Outlook Web App (OWA) uses the value of the LegacyExchangeDN attribute. If a user cannot be located using the LegacyExchangeDN value then the delivery of email messages may fail with a

5.1.1.1 NDR.

- UserPrincipalName: UPN will align to the user's NEW identity or target company (for example, user@northwindtraders.onmicrosoft.com).
- Primary SMTPAddress: Primary SMTP address will align to the user's NEW company (for example, user@northwind.com).
- TargetAddress/ExternalEmailAddress: MailUser will reference the user's current mailbox hosted in source tenant (for example user@contoso.onmicrosoft.com). When assigning this value, verify that you have/are also assigning PrimarySMTPAddress or this value will set the PrimarySMTPAddress, which will cause move failures.
- You can't add legacy smtp proxy addresses from source mailbox to target MailUser. For example, you can't maintain contoso.com on the MEU in fabrikam.onmicrosoft.com tenant objects). Domains are associated with one Azure AD or Exchange Online tenant only.

Example **target** MailUser object:

ATTRIBUTE	VALUE
Alias	LaraN
RecipientType	MailUser
RecipientTypeDetails	MailUser
UserPrincipalName	LaraN@northwintraders.onmicrosoft.com
PrimarySmtpAddress	Lara.Newton@northwind.com
ExternalEmailAddress	SMTP:LaraN@contoso.onmicrosoft.com
ExchangeGuid	1ec059c7-8396-4d0b-af4e-d6bd4c12a8d8
LegacyExchangeDN	/o=First Organization/ou=Exchange Administrative Group
	(FYDIBOHF23SPDLT)/cn=Recipients/cn=74e5385fce4b46d19006876949855035Lara
EmailAddresses	x500:/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c8190
	7273f1f9-Lara
	smtp:LaraN@northwindtraders.onmicrosoft.com
	SMTP:Lara.Newton@northwind.com

Example **source** Mailbox object:

ATTRIBUTE	VALUE
Alias	LaraN

ATTRIBUTE	VALUE
RecipientType	UserMailbox
RecipientTypeDetails	UserMailbox
UserPrincipalName	LaraN@contoso.onmicrosoft.com
PrimarySmtpAddress	Lara.Newton@contoso.com
ExchangeGuid	1ec059c7-8396-4d0b-af4e-d6bd4c12a8d8
LegacyExchangeDN	/o=First Organization/ou=Exchange Administrative Group
	(FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9Lara
EmailAddresses	smtp:LaraN@contoso.onmicrosoft.com
	SMTP:Lara.Newton@contoso.com

- Additional attributes may be included in Exchange hybrid write-back already. If not, they should be included.
 - msExchBlockedSendersHash – Writes back online safe and blocked sender data from clients to on-premises Active Directory.
 - msExchSafeRecipientsHash – Writes back online safe and blocked sender data from clients to on-premises Active Directory.
 - msExchSafeSendersHash – Writes back online safe and blocked sender data from clients to on-premises Active Directory.
2. If the source mailbox Recoverable Items size is greater than our database default (30 GB), moves will not proceed since the target quota is less than the source mailbox size. You can update the target MailUser object to transition the ELC mailbox flags from the source environment to the target, which triggers the target system to expand the quota of the MailUser to 100 GB, thus allowing the move to the target. In a Hybrid environment you will need set the appropriate msExchELCMailboxFlags on the target ADUser.
 3. Non-hybrid target tenants can modify the quota on the Recoverable Items folder for the MailUsers prior to migration by running the following command to enable Litigation Hold on the target MailUser object and increasing the quota to 100 GB:

```
Set-MailUser -Identity <MailUserIdentity> -EnableLitigationHoldForMigration
```

Note this will not work for tenants in hybrid.

4. Users in the target organization must be licensed with appropriate Exchange Online subscriptions applicable for the organization. You may apply a license in advance of a mailbox move but ONLY once the target MailUser is properly set up with ExchangeGUID and proxy addresses. Applying a license before the ExchangeGUID is applied will result in a new mailbox provisioned in target organization.

NOTE

When you apply a license on a Mailbox or MailUser object, all SMTP type proxyAddresses are scrubbed to ensure only verified domains are included in the Exchange EmailAddresses array.

5. You must ensure that the target MailUser has no previous ExchangeGuid that does not match the Source ExchangeGuid. This might occur if the target MEU was previously licensed for Exchange Online and provisioned a mailbox. If the target MailUser was previously licensed for or had an ExchangeGuid that does not match the Source ExchangeGuid, you need to perform a cleanup of the cloud MEU. For these cloud MEUs, you can run `Set-User <identity> -PermanentlyClearPreviousMailboxInfo`.

Caution

This process is irreversible. If the object has a softDeleted mailbox, it cannot be restored after this point. Once cleared, however, you can synchronize the correct ExchangeGuid to the target object and MRS will connect the source mailbox to the newly created target mailbox. (Reference EHLO blog on the new parameter.)

Find objects that were previously mailboxes using this command.

```
Get-User <identity> | select Name, *recipient* | Format-Table -AutoSize
```

Here is an example.

```
Get-User John@northwindtraders.com |select name, *recipient*| Format-Table -AutoSize
```

Name	PreviousRecipientTypeDetails	RecipientType	RecipientTypeDetails
John	UserMailbox	MailUser	MailUser

Clear the soft-deleted mailbox using this command.

```
Set-User <identity> -PermanentlyClearPreviousMailboxInfo
```

Here is an example.

```
Set-User John@northwindtraders.com -PermanentlyClearPreviousMailboxInfo -Confirm
```

Are you sure you want to perform this action?

Delete all existing information about user "John@northwindtraders.com?". This operation will clear existing values from Previous home MDB and Previous Mailbox GUID of the user. After deletion, reconnecting to the previous mailbox that existed in the cloud will not be possible and any content it had will be unrecoverable PERMANENTLY.

Do you want to continue?

[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): Y

Perform mailbox migrations

Cross-tenant Exchange mailbox migrations are initiated from the target tenant as migration batches. This is like the way that on-boarding migration batches work when migrating from Exchange on-premises to Microsoft 365.

Create Migration batches

Here is an example migration batch cmdlet for kicking off moves.

```
New-MigrationBatch -Name T2Tbatch -SourceEndpoint target_source_7977 -CSVData
([System.IO.File]::ReadAllBytes('users.csv')) -Autostart -TargetDeliveryDomain target.onmicrosoft.com
```

Identity	Status	Type	TotalCount
-----	-----	----	-----
T2Tbatch	Syncing	ExchangeRemoteMove	1

NOTE

The email address in the CSV file must be the one specified in the target tenant (for example, userA@targettenant.onmicrosoft.com), not the one in the source tenant.

[For more information on the cmdlet click here](#)

[For some example CSV file info click here](#)

The following is a minimal example CSV file:

```
EmailAddress
userA@targettenant.onmicrosoft.com
userB@targettenant.onmicrosoft.com
userC@targettenant.onmicrosoft.com
```

Migration batch submission is also supported from the new [Exchange admin center](#) when selecting the cross-tenant option.

Update on-premises MailUsers

Once the mailbox moves from source to target, you should ensure that the on-premises mail users, in both the source and target, are updated with the new targetAddress. In the examples, the targetDeliveryDomain used in the move is **contoso.onmicrosoft.com**. Update the mail users with this targetAddress.

Frequently asked questions

Do we need to update RemoteMailboxes in source on-premises after the move?

Yes, you should update the targetAddress (RemoteRoutingAddress/ExternalEmailAddress) of the source on-premises users when the source tenant mailbox moves to target tenant. While mail routing can follow the referrals across multiple mail users with different targetAddresses, Free/Busy lookups for mail users **MUST** target the location of the mailbox user. Free/Busy lookups will not chase multiple redirects.

Do Teams meetings migrate cross-tenant?

The meetings will move, however the Teams meeting URL does not update when items migrate cross-tenant. Since the URL will be invalid in the target tenant, you will need to remove and recreate the Teams meetings.

Does the Teams chat folder content migrate cross-tenant?

No, the Teams chat folder content does not migrate cross-tenant. When a mailbox is migrated cross-tenant with this feature, only user visible content in the mailbox (email, contacts, calendar, tasks, and notes) is migrated.

How can I see just moves that are cross-tenant moves, not my onboarding and off-boarding moves?

Use the *Flags* parameter. Here is an example.

```
Get-MoveRequest -Flags "CrossTenant"
```

Can you provide example scripts for copying attributes used in testing?

NOTE

SAMPLE – AS IS, NO WARRANTY This script assumes a connection to both source mailbox (to get source values) and the target on-premises Active Directory Domain Services (to stamp the ADUser object).

```
# This will export users from the source tenant with the CustomAttribute1 = "Cross-Tenant-Project"
# These are the 'target' users to be moved to the Northwind org tenant
$outFileUsers = "$home\desktop\UsersToMigrate.txt"
$outFileUsersXML = "$home\desktop\UsersToMigrate.xml"
Get-Mailbox -Filter "CustomAttribute1 -like 'Cross-Tenant-Project'" -ResultSize Unlimited | Select-Object -
ExpandProperty Alias | Out-File $outFileUsers
$mailboxes = Get-Content $outFileUsers
$mailboxes | ForEach-Object {Get-Mailbox $_} | Select-Object
PrimarySMTPAddress, Alias, SamAccountName, FirstName, LastName, DisplayName, Name, ExchangeGuid, ArchiveGuid, LegacyE
xchangeDn, EmailAddresses | Export-Clixml $outFileUsersXML
```

```
# Copy the file $outfile to the desktop of the target on-premises then run the below to create MEU in Target
$mailboxes = Import-Clixml $home\desktop\UsersToMigrate.xml
add-type -AssemblyName System.Web
foreach ($m in $mailboxes) {
    $organization = "@contoso.onmicrosoft.com"
    $mosi = $m.Alias+$organization
    $Password = [System.Web.Security.Membership]::GeneratePassword(16,4) | ConvertTo-SecureString -
AsPlainText -Force
    $x500 = "x500:" + $m.LegacyExchangeDn
    $tmpUser = New-MailUser -MicrosoftOnlineServicesID $mosi -PrimarySmtpAddress $mosi -ExternalEmailAddress
$m.PrimarySmtpAddress -FirstName $m.FirstName -LastName $m.LastName -Name $m.Name -DisplayName
$m.DisplayName -Alias $m.Alias -Password $Password
    $tmpUser | Set-MailUser -EmailAddresses @{add=$x500} -ExchangeGuid $m.ExchangeGuid -ArchiveGuid
$m.ArchiveGuid -CustomAttribute1 "Cross-Tenant-Project"
    $tmpx500 = $m.EmailAddresses | ?{$_ -match "x500"}
    $tmpx500 | %{Set-MailUser $m.Alias -EmailAddresses @{add="$_"}}
}
```

```
# Now sync the changes from On-Premises to Azure and Exchange Online in the Target tenant
# This action should create the target mail enabled users (MEUs) in the Target tenant
Start-ADSyncSyncCycle
```

How do we access Outlook on Day 1 after the user mailbox is moved?

Since only one tenant can own a domain, the former primary SMTPAddress will not be associated to the user in the target tenant when the mailbox move completes; only those domains associated with the new tenant. Outlook uses the user's new UPN to authenticate to the service and the Outlook profile expects to find the legacy primary SMTPAddress to match the mailbox in the target system. Since the legacy address is not in the target System the outlook profile will not connect to find the newly moved mailbox.

For this initial deployment, users will need to rebuild their profile with their new UPN, primary SMTP address and resync OST content.

NOTE

Plan accordingly as you batch your users for completion. You need to account for network utilization and capacity when Outlook client profiles are created and subsequent OST and OAB files are downloaded to clients.

What Exchange RBAC roles do I need to be member of to set up or complete a cross-tenant move?

There is a matrix of roles based on assumption of delegated duties when executing a mailbox move. Currently,

two roles are required:

- The first role is for a one-time setup task that establishes the authorization of moving content into or out of your tenant/organizational boundary. As moving data out of your organizational control is a critical concern for all companies, we opted for the highest assigned role of Organization Administrator (OrgAdmin). This role must alter or set up a new OrganizationRelationship that defines the - MailboxMoveCapability with the remote organization. Only the OrgAdmin can alter the MailboxMoveCapability setting, while other attributes on the OrganizationRelationship can be managed by the Federated Sharing administrator.
- The role of executing the actual move commands can be delegated to a lower-level function. The role of Move Mailboxes is assigned to the capability of moving mailboxes in or out of the organization.

How do we target which SMTP address is selected for targetAddress (TargetDeliveryDomain) on the converted mailbox (to MailUser conversion)?

Exchange mailbox moves using MRS craft the targetAddress on the original source mailbox when converting to a MailUser by matching an email address (proxyAddress) on the target object. The process takes the - TargetDeliveryDomain value passed into the move command, then checks for a matching proxy for that domain on the target side. When we find a match, the matching proxyAddress is used to set the ExternalEmailAddress (targetAddress) on the converted mailbox (now MailUser) object.

How mail flow works after migration?

Cross-Tenant mail flow after migration works similar to Exchange Hybrid mail flow. Each migrated mailbox needs the source MailUser with the correct targetaddress to forward incoming mail from source tenant to mailboxes in target tenant. Transport rules, security and compliance features will run as configured in each tenant that the mail flows through. So, for inbound mail, features like anti-spam, anti-malware, quarantine, as well as transport rules and journaling rules will run in the source tenant first, then in the target tenant.

How do mailbox permissions transition?

Mailbox permissions include Send on Behalf of and Mailbox Access:

- Send On Behalf Of (AD:publicDelegates) stores the DN of recipients with access to a user's mailbox as a delegate. This value is stored in Active Directory and currently does not move as part of the mailbox transition. If the source mailbox has publicDelegates set, you will need to restamp the publicDelegates on the target Mailbox once the MEU to Mailbox conversion completes in the target environment by running `Set-Mailbox <principle> -GrantSendOnBehalfTo <delegate>`.
- Mailbox Permissions that are stored in the mailbox will move with the mailbox when both the principal and the delegate are moved to the target system. For example, the user *TestUser_7 is granted FullAccess to the mailbox TestUser_8 in the tenant SourceCompany.onmicrosoft.com. After the mailbox move completes to TargetCompany.onmicrosoft.com, the same permissions are set up in the target directory. Examples using _Get-MailboxPermission for TestUser_7 in both source and target tenants are shown below. Exchange cmdlets are prefixed with source and target accordingly.*

Here is an example of the output of the mailbox permission before a move.

```
Get-SourceMailboxPermission TestUser_7 | Format-Table -AutoSize User, AccessRights, IsInherited, Deny
```

User	AccessRights	IsInherited	Deny
NT AUTHORITY\SELF	{FullAccess, ReadPermission}	False	False
TestUser_8@SourceCompany.onmicrosoft.com	{FullAccess}	False	False

Here's an example of the output of the mailbox permission after the move.

```
Get-TargetMailboxPermission TestUser_7 | Format-Table -AutoSize User, AccessRights, IsInherited, Deny
```

User	AccessRights	IsInherited	Deny
NT AUTHORITY\SELF	{FullAccess, ReadPermission}	False	False
TestUser_8@TargetCompany.onmicrosoft.com	{FullAccess}	False	False

NOTE

Cross-tenant mailbox and calendar permissions are NOT supported. You must organize principals and delegates into consolidated move batches so that these connected mailboxes are transitioned at the same time from the source tenant.

What X500 proxy should be added to the target MailUser proxy addresses to enable migration?

The cross-tenant mailbox migration requires that the LegacyExchangeDN value of the source mailbox object to be stamped as an x500 email address on the target MailUser object.

Example:

```
LegacyExchangeDN value on source mailbox is:
/o=First Organization/ou=Exchange Administrative
Group(FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9Lara

so, the x500 email address to be added to target MailUser object would be:
x500:/o=First Organization/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=d11ec1a2cacd4f81858c81907273f1f9-Lara
```

NOTE

In addition to this X500 proxy, you will need to copy all X500 proxies from the mailbox in the source to the mailbox in the target.

Can the source and target tenants utilize the same domain name?

No, the source tenant and target tenant domain names must be unique. For example, a source domain of contoso.com and the target domain of fourthcoffee.com.

Will shared mailboxes move and still work?

Yes, however, we only keep the store permissions as described in these articles:

- [Manage permissions for recipients in Exchange Online](#)
- [How to grant Exchange and Outlook mailbox permissions in Office 365 dedicated](#)

Do you have any recommendations for batches?

Do not exceed 2000 mailboxes per batch. We strongly recommend submitting batches two weeks prior to the cut-over date as there is no impact on the end users during synchronization. If you need guidance for mailboxes quantities over 50,000 you can reach out to the Engineering Feedback Distribution List at crosstenantmigrationpreview@service.microsoft.com.

What if I use Service encryption with Customer Key?

The mailbox will be decrypted prior to moving. Ensure Customer Key is configured in the target tenant if it is still required. See [here](#) for more information.

What is the estimated migration time?

To help you plan your migration, the table present [here](#) shows the guidelines about when to expect bulk mailbox

migrations or individual migrations to complete. These estimates are based on a data analysis of previous customer migrations. Because every environment is unique, your exact migration velocity may vary.

Do remember that this feature is currently in preview and the SLA, and any applicable Service Levels do not apply to any performance or availability issues during the preview status of this feature.

Protecting documents in the source tenant consumable by users in the destination tenant.**

Cross-tenant migration only migrates mailbox data and nothing else. There are multiple other options, which are documented in the following blog post that may help: <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/mergers-and-spinoffs/ba-p/910455>

Can I have the same labels in the destination tenant as you had in the source tenant, either as the only set of labels or an additional set of labels for the migrated users depending on alignment between the organizations.**

Because cross-tenant migrations do not export labels and there is no way to share labels between tenants, you can only achieve this by recreating the labels in the destination tenant.

Do you support moving Microsoft 365 Groups?

Currently the Cross-Tenant mailbox migrations feature does not support the migration of Microsoft 365 Groups.

Can a source tenant admin perform an eDiscovery search against a mailbox after the mailbox has been migrated to the new/target tenant?

No, after a cross tenant mailbox migration, eDiscovery against the migrated user's mailbox in the source does not work. This is because there is no longer a mailbox in the source to search against as the mailbox has been migrated to the target tenant and now belongs to the target tenant. eDiscovery, post mailbox migration can only be done in the target tenant (where the mailbox now exists). If a copy of the source mailbox needs to persist in the source tenant after migration, the admin in the source can copy the contents to an alternate mailbox pre migration for future eDiscovery operations against the data.

At which point will the destination MailUser be converted to a destination mailbox and the source mailbox converted to a source MailUser?

These conversions happen automatically during the migration process. No manual steps are necessary.

At which step should I assign the Exchange Online license to destination MailUsers?

This can be done before the migration is complete, but you should not assign a license prior to stamping the *ExchangeGuid* attribute or the conversion of MailUser object to mailbox will fail and a new mailbox will be created instead. To mitigate this risk, it is best to wait until after the migration is complete, and assign licenses during the 30 day grace period.

Can I use Azure AD Connect to sync users to the new tenant if I am keeping the on-prem Active Directory?

Yes. It is possible to have two instances of Azure AD Connect synchronize to different tenants. However, there are some things you need to be aware of.

- Preprovisioning the user's accounts with the script provided in this article should not be done. Instead, a selective OU sync of the users in scope for the migration can be performed to populate the target tenant; you will receive a warning about the UPN not matching during Azure AD Connect configuration.
- Depending on your current state of Hybrid Exchange, you need to verify that the on-prem directory objects have the required attributes (such as msExchMailboxGUID and proxyAddresses) populated correctly before attempting to sync to another tenant, or you will run into issues with double mailboxes and migration failures.
- You need to take some extra steps to manage UPN transitioning, changing it on-prem once the migration has been completed for a user unless you are also moving the custom domain during a cut-over migration.

Known issues

- **Issue: Post migration Teams functionality in the source tenant will be limited.** After the mailbox is migrated to the target tenant, Teams in the source tenant will no longer have access to the user's mailbox. So, if a user logs into Teams with the source tenant credential, then there will be a loss of functionality such as the inability to update your profile picture, no calendar application, and an inability to search and join public teams.
- **Issue: Auto Expanded archives cannot be migrated.** The cross-tenant migration feature supports migrations of the primary mailbox and archive mailbox for a specific user. If the user in the source however has an auto expanded archive – meaning more than one archive mailbox, the feature is unable to migrate the additional archives and should fail.
- **Issue: Cloud MailUsers with non-owned smtp proxyAddress block MRS moves background.** When creating target tenant MailUser objects, you must ensure that all SMTP proxy addresses belong to the target tenant organization. If an SMTP proxyAddress exists on the target mail user that does not belong to the local tenant, the conversion of the MailUser to Mailbox is prevented. This is due to our assurance that mailbox objects can only send mail from domains for which the tenant is authoritative (domains claimed by the tenant):
 - When you synchronize users from on-premises using Azure AD Connect, you provision on-premises MailUser objects with ExternalEmailAddress pointing to the source tenant where the mailbox exists (LaraN@contoso.onmicrosoft.com) and you stamp the PrimarySMTPAddress as a domain that resides in the target tenant (Lara.Newton@northwind.com). These values synchronize down to the tenant and an appropriate mail user is provisioned and ready for migration. An example object is shown here.

```
Get-MailUser LaraN | select ExternalEmailAddress, EmailAddresses

ExternalEmailAddress      EmailAddresses
-----
SMTP:LaraN@contoso.onmicrosoft.com {SMTP:lara.newton@northwind.com}
```

NOTE

The *contoso.onmicrosoft.com* address is *not* present in the EmailAddresses / proxyAddresses array.

- **Issue: MailUser objects with "external" primary SMTP addresses are modified / reset to "internal" company claimed domains**

MailUser objects are pointers to non-local mailboxes. In the case for cross-tenant mailbox migrations, we use MailUser objects to represent either the source mailbox (from the target organization's perspective) or target mailbox (from the source organization's perspective). The MailUsers will have an ExternalEmailAddress (targetAddress) that points to the smtp address of the actual mailbox (ProxyTest@fabrikam.onmicrosoft.com) and primarySMTP address that represents the displayed SMTP address of the mailbox user in the directory. Some organizations choose to display the primary SMTP address as an external SMTP address, not as an address owned/verified by the local tenant (such as fabrikam.com rather than as contoso.com). However, once an Exchange service plan object is applied to the MailUser via licensing operations, the primary SMTP address is modified to show as a domain verified by the local organization (contoso.com). There are two potential reasons:

- When any Exchange service plan is applied to a MailUser, the Azure AD process starts to enforce proxy scrubbing to ensure that the local organization is not able to send mail out, spoof, or mail from another tenant. Any SMTP address on a recipient object with these service plans will be removed if the address is not verified by the local organization. As is the case in the example, the Fabikam.com domain is NOT verified by the contoso.onmicrosoft.com tenant, so the scrubbing

removes that fabrikam.com domain. If you wish to persist these external domains on MailUser, either before the migration or after migration, you need to alter your migration processes to strip licenses after the move completes or before the move to ensure that the users have the expected external branding applied. You will need to ensure that the mailbox object is properly licensed to not affect mail service.

- An example script to remove the service plans on a MailUser in the contoso.onmicrosoft.com tenant is shown here.

```
$LO = New-MsolLicenseOptions -AccountSkuId "contoso:ENTERPRISEPREMIUM" DisabledPlans
"LOCKBOX_ENTERPRISE","EXCHANGE_S_ENTERPRISE","INFORMATION_BARRIERS","MIP_S_CLP2","MIP_S_CLP1",
"MYANALYTICS_P2","EXCHANGE_ANALYTICS","EQUIVIO_ANALYTICS","THREAT_INTELLIGENCE","PAM_ENTERPRIS
E","PREMIUM_ENCRYPTION"
Set-MsolUserLicense -UserPrincipalName ProxyTest@contoso.com LicenseOptions $lo
```

Results in the set of ServicePlans assigned are shown here.

```
(Get-MsolUser -UserPrincipalName ProxyTest@contoso.com).licenses | Select-Object -
ExpandProperty ServiceStatus |sort ProvisioningStatus -Descending
```

ServicePlan	ProvisioningStatus
ATP_ENTERPRISE	PendingProvisioning
MICROSOFT_SEARCH	PendingProvisioning
INTUNE_0365	PendingActivation
PAM_ENTERPRISE	Disabled
EXCHANGE_ANALYTICS	Disabled
EQUIVIO_ANALYTICS	Disabled
THREAT_INTELLIGENCE	Disabled
LOCKBOX_ENTERPRISE	Disabled
PREMIUM_ENCRYPTION	Disabled
EXCHANGE_S_ENTERPRISE	Disabled
INFORMATION_BARRIERS	Disabled
MYANALYTICS_P2	Disabled
MIP_S_CLP1	Disabled
MIP_S_CLP2	Disabled
ADALLOM_S_0365	PendingInput
RMS_S_ENTERPRISE	Success
YAMMER_ENTERPRISE	Success
PROJECTWORKMANAGEMENT	Success
BI_AZURE_P2	Success
WHITEBOARD_PLAN3	Success
SHAREPOINTENTERPRISE	Success
SHAREPOINTWAC	Success
KAIZALA_STANDALONE	Success
OFFICESUBSCRIPTION	Success
MCSTANDARD	Success
Deskless	Success
STREAM_0365_E5	Success
FLOW_0365_P3	Success
POWERAPPS_0365_P3	Success
TEAMS1	Success
MCOEV	Success
MCMEETADV	Success
BPOS_S_TODO_3	Success
FORMS_PLAN_E5	Success
SWAY	Success

The user's PrimarySMTPAddress is no longer scrubbed. The fabrikam.com domain is not owned by the contoso.onmicrosoft.com tenant and will persist as the primary SMTP address shown in the directory.

Here is an example.

```
Get-Recipient ProxyTest | Format-Table -AutoSize UserPrincipalName, PrimarySmtpAddress,
ExternalEmailAddress, ExternalDirectoryObjectId
UserPrincipalName           PrimarySmtpAddress           ExternalEmailAddress
ExternalDirectoryObjectId
-----
ProxyTest@fabrikam.com       ProxyTest@fabrikam.com       SMTP:ProxyTest@fabrikam.com
e2513482-1d5b-4066-936a-cbc7f8f6f817
```

- When `msExchRemoteRecipientType` is set to 8 (DeprovisionMailbox), for on-premises MailUsers that are migrated to the target tenant, the proxy scrubbing logic in Azure will remove non-owned domains and reset the primarySMTP to an owned domain. By clearing `msExchRemoteRecipientType` in the on-premises MailUser, the proxy scrub logic no longer applies.

Below is the full set of current service plans that include Exchange Online.

NAME
eDiscovery (Premium) Storage (500 GB)
Customer Lockbox
Data Loss Prevention
Exchange Enterprise CAL Services (EOP, DLP)
Exchange Essentials
Exchange Foundation
Exchange Online (P1)
Exchange Online (Plan 1)
Exchange Online (Plan 2)
Exchange Online Archiving for Exchange Online
Exchange Online Archiving for Exchange Server
Exchange Online Inactive User Add-on
Exchange Online Kiosk
Exchange Online Multi-Geo
Exchange Online Plan 1
Exchange Online POP
Exchange Online Protection

NAME
Graph Connectors Search with Index
Information Barriers
Information Protection for Office 365 - Premium
Information Protection for Office 365 - Standard
Insights by MyAnalytics
Microsoft Information Governance
Microsoft Purview Audit (Premium)
Microsoft Bookings
Microsoft Business Center
Microsoft Data Investigations
Microsoft MyAnalytics (Full)
Microsoft Communications Compliance
Microsoft Communications DLP
Microsoft Customer Key
Microsoft 365 Advanced Auditing
Microsoft Records Management
Office 365 eDiscovery (Premium)
Office 365 Advanced eDiscovery
Microsoft Defender for Office 365 (Plan 1)
Microsoft Defender for Office 365 (Plan 2)
Office 365 Privileged Access Management
Premium Encryption in Office 365

Cross-Tenant Identity Mapping (preview)

10/28/2022 • 3 minutes to read • [Edit Online](#)

Cross-Tenant Identity Mapping is a feature that can be used during migrations from one Microsoft 365 organization to another (commonly referred to as a cross-tenant migration). It provides a secure method of establishing one-to-one object relationships across organization boundaries and automatically prepares the target objects for a successful migration.

NOTE

Cross-Tenant Identity Mapping is in a private preview stage of development. As an unfinished project any information or availability is subject to change at any time. Support for private-preview customers will be handled via email. Cross-Tenant Identity Mapping is covered by the **preview terms** of the [Microsoft Universal License Terms for Online Services](#).

Benefits of using Cross-Tenant Identity Mapping

Cross-Tenant Identity Mapping removes the need to export large data sets from a source organization for the sole purpose of configuring Mail Enabled User objects in the target organization.

With Cross-Tenant Identity Mapping, data remains within the Microsoft security boundary and is securely copied directly from the source organization to the target organization using specially configured **Organization Relationships** serving as a unidirectional trust.

Using Cross-Tenant Identity Mapping will reduce the potential for mistakes when configuring what could potentially be thousands of target objects for a migration by automatically configuring values such as *ExchangeGuid*, *ArchiveGuid*, and all necessary *X500 proxy addresses*.

Some additional benefits of using Cross-Tenant Identity Mapping:

- Reduces the number of manual processes where a mistake may result in failed migrations
- Automates identification of objects within scope to migrate from the source organization to the target organization
- Establishes a 1:1 map of a Mailbox User object in the source organization to a pre-existing Mail Enabled User object in the target organization
- Automates population of required attributes from the source organization Mailbox User to the target organization Mail Enabled User
- Provides a list of objects prepared and ready for [cross-tenant mailbox migration](#) based on the source organization users' primarySMTPAddress value

FAQ about Cross-Tenant Identity Mapping

We would like to provide information commonly asked so you may evaluate if you would like to participate in the private preview.

- The feature is only intended to be used with [Cross-tenant mailbox migration \(preview\)](#), and not with any third-party non-Microsoft migration solutions.
- Data processing (storage, compute, transfer, etc.) is currently within the United States of America, and within the Exchange Online home region of the organizations participating in the migration.
 - For Multi-Geo enabled organizations, the organization's home geo for Exchange Online will be used.
- This feature can currently only be enabled in the worldwide Microsoft 365 offering. It doesn't work in GCC,

GCC High, DoD, Office 365 by 21 Vianet, etc.

- Some familiarity with PowerShell is currently required as the feature is PowerShell-based
- The feature communicates over an encrypted connection to a REST endpoint.
- The feature currently requires the Global Administrator role for initial setup. This behavior may change in a future update.
- Organizational Relationships are used as a dual handshake approach to ensure both organizations have authorized this transaction type to take place.
- It works with cloud-only or hybrid organizations.
- Target organizations in a hybrid configuration will require an on-premises Exchange server to modify any Mail Enabled User objects synchronized from the on-premises directory. We haven't tested support for the new Exchange Management Tool feature released in Exchange Server 2019 CU12.

What does participating in the private preview entail?

We're looking for customers willing to both try Cross-Tenant Identity Mapping and to provide feedback based on their experience. Did it make the migration easier for you compared to earlier migrations you've performed? Are there features you feel are missing? All constructive feedback is welcomed.

How to participate

If you would like to participate or you have more questions, please email CTIMPreview@service.microsoft.com and provide some basic information about the migration you would like to use Cross-Tenant Identity Mapping with.

Next steps

We recommend reviewing the current Cross-Tenant Mailbox Migration steps related to preparing target user objects for migration as this preparation is what Cross-Tenant Identity Mapping will automate.

- [Review Cross-Tenant Mailbox Migration \(preview\)](#)

Cross-tenant OneDrive migration

10/28/2022 • 2 minutes to read • [Edit Online](#)

NOTE

Information in this article refers to **Cross-tenant OneDrive migration**. [Learn about about the cross-tenant Mailbox migration here](#)

During mergers or divestitures, you commonly need the ability to move your user OneDrive accounts into a new Microsoft 365 tenant. With Cross-tenant OneDrive migration, tenant administrators can use familiar tools like *SharePoint Online PowerShell* to transition users into their new organization.

SharePoint administrators of two separate tenants can use the *Set-SPOCrossTenantRelationship* cmdlet to establish an organization relationship, and the *Start-SPOCrossTenantUserContentMove* command to begin Cross-tenant OneDrive moves.

Up to 4,000 OneDrive accounts can be scheduled for migration in advance at a given time. Once scheduled, migrations occur without the user's data ever leaving the Microsoft 365 cloud and with minimal disruption, requiring only a few minutes where a user's OneDrive will be read-only. When migrations are complete, a redirect is placed in the location of the user's original OneDrive, so any links to files and folders can continue working in the new location.

IMPORTANT

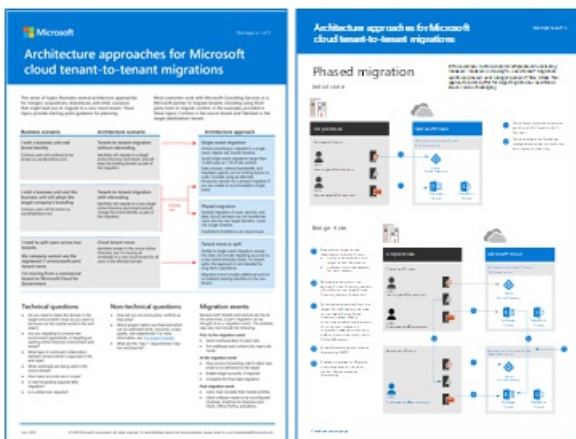
- Each user having their OneDrive migrated cross-tenant must be licensed for Cross-tenant User Data Migration.
- Cross-tenant OneDrive migration cannot be used for customers using Service Encryption with Microsoft Purview Customer Key. [Learn about Service encryption with Microsoft Purview Customer Key - Microsoft Purview](#)

Microsoft 365 tenant-to-tenant migrations

10/28/2022 • 2 minutes to read • [Edit Online](#)

There are several architecture approaches for mergers, acquisitions, divestitures, and other scenarios that might lead you to migrate an existing Microsoft 365 tenant to a new tenant. Most customers work with Microsoft Consulting Services or a Microsoft partner to migrate tenants, including using third-party tools to migrate content.

Use the [Tenant-to-tenant migration architecture model](#) to understand how to plan for Microsoft 365 tenant-to-tenant migrations and the steps of a migration.



You download this model in [PDF](#) format and print it on letter, legal, or tabloid (11 x 17) size paper.

This model provides guidance and a starting-point for planning with sections on:

- Mapping of business scenarios to architecture approaches
- Design considerations

This model also contains detailed examples of:

- A single event migration flow
- A phased migration flow
- A tenant move or split flow

Microsoft 365 Multi-Geo

10/28/2022 • 4 minutes to read • [Edit Online](#)

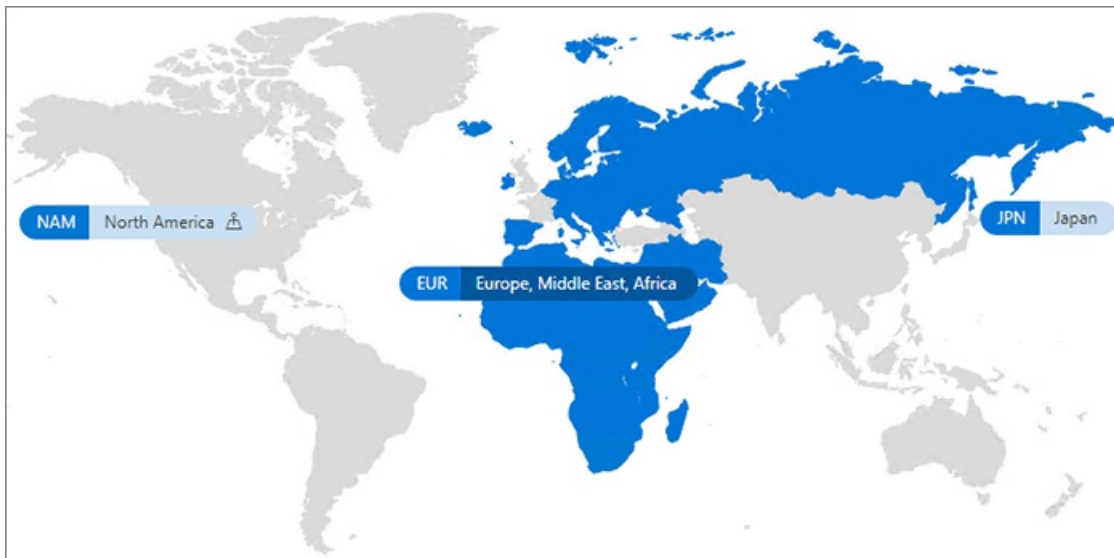
With Microsoft 365 Multi-Geo, your organization can expand its Microsoft 365 presence to multiple geographic regions and/or countries within your existing tenant. Reach out to your Microsoft Account Team to sign up your Multi-National Company for Microsoft 365 Multi-Geo.

With Microsoft 365 Multi-Geo, you can provision and store data at rest in the geo locations that you've chosen to meet data residency requirements, and at the same time unlock your global roll out of modern productivity experiences to your workforce.

For a video introduction to Microsoft 365 Multi-Geo, see [SharePoint Online and OneDrive Multi-Geo to control where your data resides](#).

Multi-Geo architecture

In a Multi-Geo environment, your Microsoft 365 tenant consists of a central location (where your Microsoft 365 subscription was originally provisioned) and one or more satellite locations. In a multi-geo tenant, the information about geo locations, groups, and user information, is mastered in Azure Active Directory (Azure AD). Because your tenant information is mastered centrally and synchronized into each geo location, sharing and experiences involving anyone from your company contain global awareness.



Note that Microsoft 365 Multi-Geo is not designed for performance optimization, it is designed to meet data residency requirements. For information about performance optimization for Microsoft 365, see [Network planning and performance tuning for Microsoft 365](#) or contact your support group.

Terminology

Here are the key terms used in describing Microsoft 365 Multi-Geo:

- **Central location** - the geo location where your tenant was originally provisioned.
- **Geo administrator** - An administrator who can administer one or more specified satellite locations.
- **Geo code** - a three-letter code for a given geo location.
- **Geo location** – A geographic location that can be used in a multi-geo tenant to host data, including Exchange mailboxes and OneDrive and SharePoint sites.

- **Preferred Data Location (PDL)** – A user property set by the administrator that indicates where the geo location where the users Exchange mailbox and OneDrive should be provisioned. The PDL also determines where SharePoint sites that are created by the user are provisioned.
- **Satellite location** – The geo locations where the geo-aware Microsoft 365 workloads (SharePoint, OneDrive, and Exchange) are enabled in a multi-geo tenant.
- **Tenant** – An organization's representation in Microsoft 365 which typically has one or more domains associated with it (for example, contoso.com).

Licensing

Microsoft 365 Multi-Geo is available as an add-on to the following Microsoft 365 subscription plans for Enterprise Agreement customers with a minimum of 250 Microsoft 365 seats in their tenant, and a minimum of 5% of those seats using multi-geo. User subscription licenses must be on the same Enterprise Agreement as the Multi-Geo Services licenses. Please contact your Microsoft account team for details.

- Microsoft 365 F1, F3, E3, or E5
- Office 365 F3, E1, E3, or E5
- Exchange Online Plan 1 or Plan 2
- OneDrive for Business Plan 1 or Plan 2
- SharePoint Online Plan 1 or Plan 2

If a license is assigned to a user and later removed, Teams user chat data is queued to be moved back to the central location. SharePoint and Exchange data is not moved.

Microsoft 365 Multi-Geo availability

Microsoft 365 Multi-Geo is currently offered in these regions and countries:

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Asia-Pacific	APC	Southeast or East Asia datacenters
Australia	AUS	Southeast or East Asia datacenters
Brazil	BRA	(eDiscovery data location coming soon)
Canada	CAN	US datacenters
Europe / Middle East / Africa	EUR	Europe datacenters
France	FRA	Europe datacenters
Germany	DEU	Europe datacenters
India	IND	Southeast or East Asia datacenters
Japan	JPN	Southeast or East Asia datacenters
Korea	KOR	Southeast or East Asia datacenters
North America	NAM	US datacenters

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Norway	NOR	(eDiscovery data location coming soon)
Qatar	QAT	(eDiscovery data location coming soon)
South Africa	ZAF	Europe datacenters
Sweden	SWE	Europe datacenters
Switzerland	CHE	Europe datacenters
United Arab Emirates	ARE	Southeast or East Asia datacenters
United Kingdom	GBR	Europe datacenters

Getting started

Follow these steps to get started with multi-geo:

1. Work with your account team to add the *Multi-Geo Capabilities in Microsoft 365* service plan. They will guide you to add the number of licenses needed. Multi-Geo feature is available to EA customers with a minimum of 250 Microsoft 365 subscriptions.

Before you can start using Microsoft 365 Multi-Geo, Microsoft needs to configure your Exchange Online tenant for multi-geo support. This one-time configuration process is triggered after you order the *Multi-Geo Capabilities in Microsoft 365* service plan and the licenses show up in your tenant. You will receive workload-specific notifications in the [Microsoft 365 message center](#) once your tenant has completed the configuration process for each workload, and you then may begin configuring and using your Microsoft 365 Multi-Geo capabilities. The time required to configure a tenant for Multi-Geo support varies from tenant to tenant, but most tenants finish within a month after receipt of the feature licenses. Larger or more complex tenants may require more time to complete the configuration process. Please contact your account team for details on your specific tenant should you require it.

2. Read [Plan your multi-geo environment](#).
3. Learn about [administering a multi-geo environment](#) and [how your users will experience the environment](#).
4. When you are ready to set up Microsoft 365 Multi-Geo, [configure your tenant for multi-geo](#).
5. [Set up search](#).

See also

[Multi-Geo in Exchange Online and OneDrive](#)

[Multi-Geo Capabilities in OneDrive and SharePoint Online](#)

[Multi-Geo Capabilities in Exchange Online](#)

[Teams experience in a multi-geo environment](#)

Multi-Geo capabilities in Microsoft Teams

10/28/2022 • 2 minutes to read • [Edit Online](#)

Multi-Geo capabilities in Teams enable Teams chat data to be stored at rest in a specified geo location. Chat data consists of chat messages, including private messages, channel messages, and images used in chats.

Teams uses the Preferred Data Location (PDL) for users and groups to determine where to store data. If the PDL isn't set or is invalid, data is stored in the tenant's central location.

NOTE

Multi-Geo capabilities in Teams rolled out in July 2021. Your chat and channel messages will be automatically migrated to the correct geo location over the next few quarters. Any new PDL changes will be processed after the tenant has completed the initial sync, and new PDL changes beyond that will be queued and processed in the order they are received.

User chat

User chat includes one-to-one, one-to-many, and private meeting messages.

When a new user is created, Teams reads the user's PDL and stores all their chat data in that geo location.

For existing users, if an administrator adds or modifies the PDL for a user, that user's chat data is added to a migration queue to be moved to the specified geo location.

The storage location for a one-to-one or one-to-many chat is based on the PDL of the person who created the chat. If that user's PDL is changed, the chat will be migrated to the new geo location. The storage location for a meeting chat is based on the PDL of the meeting organizer.

To find the current location of a user's Teams data, [connect to Teams PowerShell](#) and run the following command:

```
Get-MultiGeoRegion -EntityType User -EntityId <UPN>
```

Channel messages

Each Microsoft 365 group has a Preferred Data Location (PDL) which denotes the geo location where related data is to be stored. Teams uses the PDL for the group associated with each team to determine where to store channel messaging data for that team. This includes private channels and chat that occurs within a channel meeting.

When a user creates a new team, that user's PDL determines what PDL is assigned to the Microsoft 365 group. The group PDL determines where that team's data is stored. If that user's PDL later changes, the group's PDL isn't changed.

For existing teams, if an administrator adds or modifies the PDL for the Microsoft 365 group that backs a team, that team's channel messaging data is added to a migration queue to be moved to the specified geo location.

Changing the PDL of the Microsoft 365 group queues the Teams data to migrate to the chosen location. However, this doesn't migrate the SharePoint site or files associated with the Group automatically. You must move the site separately by following the procedures in [Move a SharePoint site to a different geo location](#). Be

sure to do both steps to avoid Teams data and SharePoint data for one group in different locations.

To find the current location of a team's data, [connect to Teams PowerShell](#) and run the following command:

```
Get-MultiGeoRegion -EntityType Group -EntityId <GroupId>
```

User Experience

Teams Multi-Geo is seamless to the end user. Once you change the PDL of a user or a group, the respective data will queue for migration and the migration will occur automatically with no impact to the user or their Teams client even if they're active while the migration occurs.

See also

[Microsoft 365 Multi-Geo tenant configuration](#)

[Administering a multi-geo environment](#)

[Administering Exchange Online mailboxes in a multi-geo environment](#)

Multi-Geo Capabilities in OneDrive and SharePoint Online

10/28/2022 • 2 minutes to read • [Edit Online](#)

Multi-Geo capabilities in OneDrive and SharePoint Online enable control of shared resources like SharePoint team sites and Microsoft 365 Group mailboxes stored at rest in a specified geo location.

Each user, Group mailbox, and SharePoint site have a Preferred Data Location (PDL) which denotes the geo location where related data is to be stored. Users' personal data (Exchange mailbox and OneDrive) along with any Microsoft 365 Groups or SharePoint sites that they create can be stored in the specified geo location to meet data residency requirements. You can [specify different administrators for each geo location](#).

Users get a seamless experience when using Microsoft 365 services, including Office applications, OneDrive, and Search. See [User experience in a multi-geo environment](#) for details.

OneDrive

Each user's OneDrive can be provisioned in or [moved by an administrator](#) to a satellite location in accordance with the user's PDL. Personal files are then kept in that geo location, though they can be shared with users in other geo locations.

SharePoint Sites and Groups

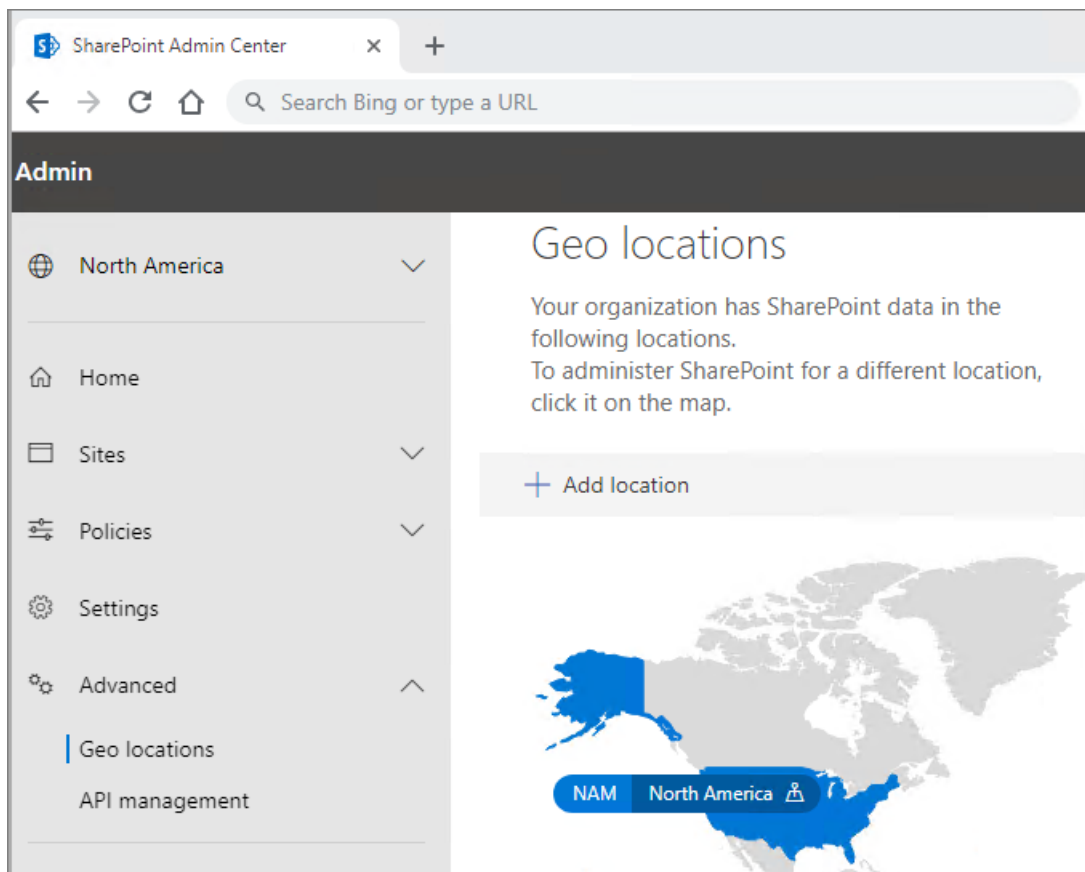
Management of the Multi-Geo feature is available through the [SharePoint admin center](#). Detailed information can be found in the [corresponding blog post](#).

When a user creates a SharePoint group-connected site in a multi-geo environment, their PDL is used to determine the geo location where the site and its associated Group mailbox are created. (If the user's PDL value hasn't been set, or has been set to geo location that hasn't been configured as a satellite location, then the site and mailbox are created in the central location.)

Microsoft 365 services other than Exchange, OneDrive, SharePoint, and Teams aren't Multi-Geo. However, Microsoft 365 Groups that are created by these services will be configured with the PDL of the creator and their Exchange Group mailbox, SharePoint site are provisioned in the corresponding geo.

Managing the multi-geo environment

Setting up and managing your multi-geo environment is done through the [SharePoint admin center](#).



(Some actions, such as moving a SharePoint site or a OneDrive site require Microsoft PowerShell.)

See also

[Multi-Geo in SharePoint and Microsoft 365 Groups](#)

[Administering a multi-geo environment](#)

[SharePoint storage quotas in multi-geo environments](#)

[Administering Exchange Online mailboxes in a multi-geo environment](#)

Multi-Geo Capabilities in Exchange Online

10/28/2022 • 3 minutes to read • [Edit Online](#)

In a multi-geo environment, you can select the location of Exchange Online mailbox content (data at rest) on a per-user basis.

You can place mailboxes in satellite geo locations by:

- Creating a new Exchange Online mailbox directly in a satellite geo location.
- Moving an existing Exchange Online mailbox to a satellite geo location by changing the user's preferred data location.
- Onboarding a mailbox from an on-premises Exchange organization directly into a satellite geo location.

Mailbox placement and moves

After Microsoft completes the prerequisite multi-geo configuration steps, Exchange Online will honor the **PreferredDataLocation** attribute on user objects in Azure AD.

Exchange Online synchronizes the **PreferredDataLocation** property from Azure AD into the **MailboxRegion** property in the Exchange Online directory service. The value of **MailboxRegion** determines the geo location where user mailboxes and any associated archive mailboxes will be placed. It is not possible to configure a user's primary mailbox and archive mailboxes to reside in different geo locations. Only one geo location may be configured per user object.

- When **PreferredDataLocation** is configured on a user with an existing mailbox, the mailbox will be put into a relocation queue and automatically moved to the specified geo location.
- When **PreferredDataLocation** is configured on a user without an existing mailbox, when you provision the mailbox, it will be provisioned into the specified geo location.
- When **PreferredDataLocation** is not specified on a user, when you provision the mailbox, it will be provisioned in the central geo location.
- If the **PreferredDataLocation** code is incorrect (e.g. a typo of NAN instead of NAM), the mailbox will be provisioned in the central geo location.

Note: Multi-geo capabilities and Skype for Business Online regionally hosted meetings both use the **PreferredDataLocation** property on user objects to locate services. If you configure **PreferredDataLocation** values on user objects for regionally hosted meetings, the mailbox for those users will be automatically moved to the specified geo location after multi-geo is enabled on the Microsoft 365 tenant.

Feature limitations for multi-geo in Exchange Online

- Security and compliance features (for example, auditing and eDiscovery) that are available in the Exchange admin center (EAC) aren't available in multi-geo organizations. Instead, you need to use the [Microsoft 365 Security & Compliance Center](#) to configure security and compliance features.
- Outlook for Mac users may experience a temporary loss of access to their Online Archive folder while you move their mailbox to a new geo location. This condition occurs when the user's the primary and archive mailboxes are in different geo locations, because cross-geo mailbox moves may complete at different times.

- Users can't share *mailbox folders* across geo locations in Outlook on the web (formerly known as Outlook Web App or OWA). For example, a user in the European Union can't use Outlook on the web to open a shared folder in a mailbox that's located in the United States. However, Outlook on the Web users can open *other mailboxes* in different geo locations by using a separate browser window as described in [Open another person's mailbox in a separate browser window in Outlook Web App](#).

Note: Cross-geo mailbox folder sharing is supported in Outlook on Windows.

- Public folders are supported in multi-geo organizations. However, the public folders must remain in the central geo location. You can't move public folders to satellite geo locations.
- In a multi-geo environment, cross-geo mailbox auditing is not supported. For example, if a user is assigned permissions to access a shared mailbox in a different geo location, mailbox actions performed by that user are not logged in the mailbox audit log of the shared mailbox. Exchange admin audit events are also only available for the default location. For more information, see [Manage mailbox auditing](#).

Plan for Microsoft 365 Multi-Geo

10/28/2022 • 5 minutes to read • [Edit Online](#)

This guidance is designed for administrators of multi-national companies (MNCs) who are preparing their Microsoft 365 tenant to be expanded to additional geographies in accordance with the company's presence to meet data residency requirements.

In a multi-geo configuration, your Microsoft 365 tenant consists of a central location and one or more satellite locations. This is a single tenant that spans across multiple geo locations. Your tenant information, including geo locations, is mastered in Azure Active Directory (Azure AD).

Here are some key multi-geo terms to help you understand the basic concepts of the configuration:

- **Tenant** – An organization's representation in Microsoft 365 which typically has one or more domains associated with it (for example, <https://contoso.sharepoint.com>).
- **Geo locations** – The geographic locations available to host data in a Microsoft 365 tenant.
- **Satellite locations** – The additional geo locations that you have configured to host data in your Microsoft 365 tenant. Multi-geo tenants span more than one geo location, for example, North America and Europe.
- **Preferred Data Location (PDL)** – The geo location where an individual user's Exchange and OneDrive data is stored. This can be set by the administrator to any of the geo locations that have been configured for the tenant. Note that if you change the PDL for a user who already has a OneDrive site, their OneDrive data is not moved to the new geo location automatically. See [Move a OneDrive library to a different geo-location](#) for more information. If they have an Exchange mailbox, the mailbox is moved to the new preferred data location automatically.

Enabling Multi-Geo requires four key steps:

1. Work with your account team to add the *Multi-Geo Capabilities in Microsoft 365* service plan.
2. Choose your desired satellite location(s) and add them to your tenant.
3. Set your users' preferred data location to the desired satellite location. When a new OneDrive site or Exchange mailbox is provisioned for a user, it is provisioned to their PDL.
4. Migrate your users' existing OneDrive sites from the central location to their preferred data location as needed. (Exchange mailboxes are migrated automatically when you set a user's PDL.)

See [Configure Microsoft 365 Multi-Geo](#) for details on each of these steps.

IMPORTANT

Note that Microsoft 365 Multi-Geo is not designed for performance optimization, it is designed to meet data residency requirements. For information about performance optimization for Microsoft 365, see [Network planning and performance tuning for Microsoft 365](#) or contact your support group.

You can configure any of the following locations to be satellite locations where you can host OneDrive and SharePoint sites, and Exchange mailboxes. As you plan for multi-geo, make a list of the locations that you want to add to your Microsoft 365 tenant. We recommend starting with one or two satellite locations and then gradually expanding to more geo locations, if needed.

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Asia-Pacific	APC	Southeast or East Asia datacenters
Australia	AUS	Southeast or East Asia datacenters
Brazil	BRA	(eDiscovery data location coming soon)
Canada	CAN	US datacenters
Europe / Middle East / Africa	EUR	Europe datacenters
France	FRA	Europe datacenters
Germany	DEU	Europe datacenters
India	IND	Southeast or East Asia datacenters
Japan	JPN	Southeast or East Asia datacenters
Korea	KOR	Southeast or East Asia datacenters
North America	NAM	US datacenters
Norway	NOR	(eDiscovery data location coming soon)
Qatar	QAT	(eDiscovery data location coming soon)
South Africa	ZAF	Europe datacenters
Sweden	SWE	Europe datacenters
Switzerland	CHE	Europe datacenters
United Arab Emirates	ARE	Southeast or East Asia datacenters
United Kingdom	GBR	Europe datacenters

When you configure multi-geo, consider taking the opportunity to consolidate your on-premises infrastructure while migrating to Microsoft 365. For example, if you have on-premises farms in Singapore and Malaysia, then you can consolidate them to the APC satellite location, provided data residency requirements allow you to do so.

Best practices

We recommend that you create a test user in Microsoft 365 to do some initial testing. We'll walk through some testing and verification steps with this user before you proceed to onboard production users into Microsoft 365 Multi-Geo.

Once you've completed testing with the test user, select a pilot group – perhaps from your IT department – to be the first to use OneDrive and Exchange in a new geo location. For this first group, select users who do not yet have a OneDrive. We recommend no more than five people in this initial group and gradually expand following

a batched rollout approach.

Each user should have a *preferred data location* (PDL) set so that Microsoft 365 can determine in which geo location to provision their OneDrive. The user's preferred data location must match one of your chosen satellite locations or your central location. While the PDL field is not mandatory, we recommend that a PDL be set for all users. Workloads of a user without a PDL will be provisioned in the central location.

Create a list of your users, and include their user principal name (UPN) and the location code for the appropriate preferred data location. Include your test user and your initial pilot group to start with. You'll need this list for the configuration procedures.

If your users are synchronized from an on-premises Active Directory system to Azure Active Directory, you must set the preferred data location as an Active Directory attribute and synchronize it by using Azure Active Directory Connect. You cannot directly configure the preferred data location for synchronized users using Azure AD PowerShell. The steps to set up PDL in Active Directory and Synchronize it are covered in [Azure Active Directory Connect sync: Configure preferred data location for Microsoft 365 resources](#).

The administration of a multi-geo tenant can differ from a non-multi-geo tenant, as many of the SharePoint and OneDrive settings and services are multi-geo aware. We recommend that you review [Administering a multi-geo environment](#) before you proceed with your configuration.

Read [User experience in a multi-geo environment](#) for details about your end users' experience in a multi-geo environment.

To get started configuring Microsoft 365 Multi-Geo, see [Configure Microsoft 365 Multi-Geo](#).

Once you've completed the configuration, remember to [migrate your users' OneDrive libraries](#) as needed to get your users working from their preferred data locations.

Related topics

[Microsoft 365 Multi-Geo eDiscovery configuration](#)

Administering a multi-geo environment

10/28/2022 • 4 minutes to read • [Edit Online](#)

Here's a look at how Microsoft 365 services work in a multi-geo environment.

Administrator experience

The SharePoint admin center has a [Geo locations](#) tab in the left navigation that features a geo locations map where you can view and manage your geo locations. Use this page to add or delete geo locations for your tenant.

Audit log search

A unified [Audit log](#) for all your satellite locations is available from the Microsoft 365 audit log search page. You can see all the audit log entries from across geo locations, for example, NAM & EUR users' activities will show up in one org view and then you can apply existing filters to see specific user's activities.

NOTE

Exchange admin audit events are only available for the default location.

BCS, Secure Store, Apps

BCS, Secure Store, and Apps all have separate instances in each satellite location, therefore the SharePoint Online administrator should manage and configure these services separately from each satellite location.

Compliance admin center

There is one central compliance center for a multi-geo tenant: [Microsoft Purview admin center](#).

eDiscovery

By default, an eDiscovery Manager or Administrator of a multi-geo tenant will be able to conduct eDiscovery only in the central location of that tenant. The Office 365 global administrator must assign eDiscovery Manager permissions to allow others to perform eDiscovery and assign a "Region" parameter in their applicable Compliance Security Filter to specify the region for conducting eDiscovery as satellite location, otherwise no eDiscovery will be carried out for the satellite location. To configure the Compliance Security Filter for a Region, see [Configure Office 365 Multi-Geo eDiscovery](#).

Exchange mailboxes

Users' Exchange mailboxes are moved automatically if their PDL is changed. When a new mailbox is created, it is provisioned to the user's PDL or to the central location if no value has been set for the user's PDL.

Information Protection (IP) Data Loss Prevention (DLP) policy

You can set your IP DLP policies for OneDrive for Business, SharePoint, and Exchange in the Security and Compliance center, scoping policies as needed to the whole tenant or to applicable users. For example: If you wish to select a policy for a user in a satellite location, select to apply the policy to a specific OneDrive and enter

the user's OneDrive url. See [Overview of data loss prevention policies](#) for general guidance in creating DLP policies.

The DLP policies are automatically synchronized based on their applicability to each geo location.

Implementing Information Protection and Microsoft Purview Data Loss Prevention policies to all users in a geo location is not an option available in the UI, instead you must select the applicable accounts for the policy or apply the policy globally to all accounts.

Microsoft Power Apps

Power Apps created for the satellite location will use the end point located in the central location for the tenant. Microsoft Power Apps is not a Multi-Geo service.

Power Automate

Flows created for the satellite location will use the end point located in the default geo location for the tenant. Power Automate is not a Multi-Geo service.

SharePoint storage quota

By default, all geo locations of a multi-geo environment share the available tenant storage quota. You can also manage the storage quota by allocating a specific quota for a particular geo location. For more information, see [SharePoint storage quotas in multi-geo environments](#).

Sharing

Administrators can set and manage sharing policies for each of their locations. The OneDrive and SharePoint sites in each geo location will honor only the corresponding geo-specific sharing settings. (For example, you can allow [external sharing](#) for your central location, but not for your satellite location or vice versa.) Note that the sharing settings do not allow configuring sharing limitations between geo locations.

Stream

Videos uploaded to Stream in a 1:1 chat are stored in the OneDrive of the person uploading. Meeting recordings are stored in the OneDrive of each attendee who records the meeting.

Taxonomy

We support a unified [taxonomy](#) for enterprise-managed metadata across geo locations, with the master being hosted in the central location for your company. We recommend that you manage your global taxonomy from the central location and only add location-specific terms to the satellite location's Taxonomy. Global taxonomy terms will synchronize to the satellite locations.

See [Manage metadata in a multi-geo tenant](#) for additional details and for developer guidance.

User Profile Application

There is a [user profile application](#) in each geo location. Each user's profile information is hosted in their geo location and available to the administrator for that geo location.

If you have custom profile properties, then we recommend that you use the same profile schema across geographies and populate your custom profile properties either in all geo locations or where needed. For guidance regarding how to populate user profile data programmatically, please refer to the [Bulk User Profile Update API](#).

See [Work with user profiles in a multi-geo tenant](#) for additional details and for developer guidance.

Yammer

Yammer is not a Multi-Geo workload. Yammer threads stored in Yammer will be placed in the tenant's central location. Yammer is rolling out a file storage change which will store Yammer files within SharePoint. Yammer files stored in SharePoint will be placed the SharePoint site associated with the Yammer group. SharePoint group sites are based on PDL logic as outlined in [SharePoint Sites and Groups](#).

User experience in a multi-geo environment

10/28/2022 • 4 minutes to read • [Edit Online](#)

Here's what your users will see in a OneDrive Multi-Geo configuration:

Exchange mailbox

A user's Exchange mailbox is provisioned to their preferred data location, and is automatically relocated if their PDL changes. Users can use Outlook and Outlook on the web normally with no change in user experience in a multi-geo environment.

Hub sites

SharePoint Hub sites enhance the discovery and engagement with content for employees, while creating a complete and consistent representation of projects, departments or regions. In a multi-geo environment, sites from satellite locations can easily be associated with a hub site regardless the hub site's geo location. Users can search and get results across the hub through a single search experience, regardless of the geo location of the sites.

Microsoft 365 app launcher

The app launcher is multi-geo aware and will direct each tile to the appropriate geo location of the workload. The SharePoint and OneDrive tiles will point the user to the location corresponding to the user's provisioned geo location. This means that if the user has a OneDrive in the central location, their SharePoint tile will point them to SP Home in the central location but their group site will be provisioned in the location corresponding to their PDL.

Office applications

Office applications such as Word, Excel, and PowerPoint will automatically detect the correct OneDrive geo-location for each user when they log in. Users do not need to enter the geo-specific URL for their OneDrive or SharePoint sites.

OneDrive sync app

The OneDrive sync app (version 17.3.6943.0625 and later) will automatically detect the correct OneDrive geo location for the user. Sync app support includes the ability to sync groups-based sites regardless of their geo location. The Groove sync client is not supported for multi-geo.

OneDrive location

Users will have their OneDrive provisioned in their preferred data location. If a user navigates to a OneDrive URL that contains an incorrect geo location (such as a bookmark from a previous geo location), they are automatically redirected to the OneDrive in the appropriate geo location.

OneDrive iOS and Android

The OneDrive iOS and Android mobile apps will show you your OneDrive files and files shared with you regardless of their geo location. Search from the OneDrive mobile apps will show relevant results from all geo locations. Download the latest version of these apps.

For more information, see Use [OneDrive on iOS](#) and [Use OneDrive for Android](#) for more information.

OneDrive Mobile Client

The OneDrive Mobile Client is multi-geo aware and will display pertinent content and results from all geo locations.

Search

Each geo location has its own search index and Search Center. When a user searches, the query is sent to all the geo locations, and the returned results are merged and then ranked so the user gets unified results. Users get results from all geo locations regardless of their own geo location. See [Configure Search for OneDrive Multi-Geo](#) for specifics.

The following search clients are supported:

- OneDrive
- Delve
- SharePoint Home
- The Search Center
- Custom search applications that use the SharePoint Search API

SharePoint Home

In SharePoint Multi-Geo, your SharePoint home is hosted in the location where the user resides as determined by their OneDrive location. For example: if the user has their OneDrive hosted in a European satellite location, their SharePoint Home will be rendered from Europe. SharePoint home includes all content relevant to the user regardless of its geo location.

Followed Sites, News from Sites, Recent Sites, Frequent Sites, and Suggested sites

All of these components will show up for the user regardless of the geo location where the content is hosted, so long as the user has permissions to said content.

Features Links

Admins may configure Featured links in SharePoint home as appropriate to each geo location. This allows the admin to feature in the SP Home for each region the links that are appropriate for users in the region.

SharePoint Mobile Client

The SharePoint Mobile Client is multi-geo aware and will display pertinent content and results from all geo locations.

Sharing

The People Picker experience shows all users regardless of their geo location. This allows a user to share with another user in their same geo or in any other of your tenant's geo locations. Content from different geo locations will show up in the **Shared with Me** view in the user's OneDrive, Word, Excel, PowerPoint, and Office.com and can be accessed with Single Sign-On experience regardless of which geo location it is hosted in.

Teams Experience

Teams is a multi-geo service. OneDrive files and recently viewed files are shown regardless of the user's geo

location. @ mentions work with users from all geo-locations.

User profiles

User profile information is mastered in the user's geo location. When selecting a user, you will be directed to the appropriate geo location for the user, where you will see their full profile details.

If Delve is turned off, you will see the classic profile experience in SharePoint, which is not multi-geo aware.

Microsoft 365 Multi-Geo tenant configuration

10/28/2022 • 7 minutes to read • [Edit Online](#)

Before you configure your tenant for Microsoft 365 Multi-Geo, be sure you have read [Plan for Microsoft 365 Multi-Geo](#). To follow the steps in this article, you'll need a list of the geo locations that you want to enable as satellite locations, and the test users that you want to provision for those locations.

Add the Multi-Geo Capabilities in your Microsoft 365 plan to your tenant

To use Microsoft 365 Multi-Geo, you need the *Multi-Geo Capabilities in Microsoft 365* plan. Work with your account team to add this plan to your tenant. Your account team will connect you with the appropriate licensing specialist and get your tenant configured.

Note that the *Multi-Geo Capabilities in Microsoft 365* plan are a user-level service plan. You need a license for each user that you want to host in a satellite location. You can add more licenses over time as you add users in satellite locations.

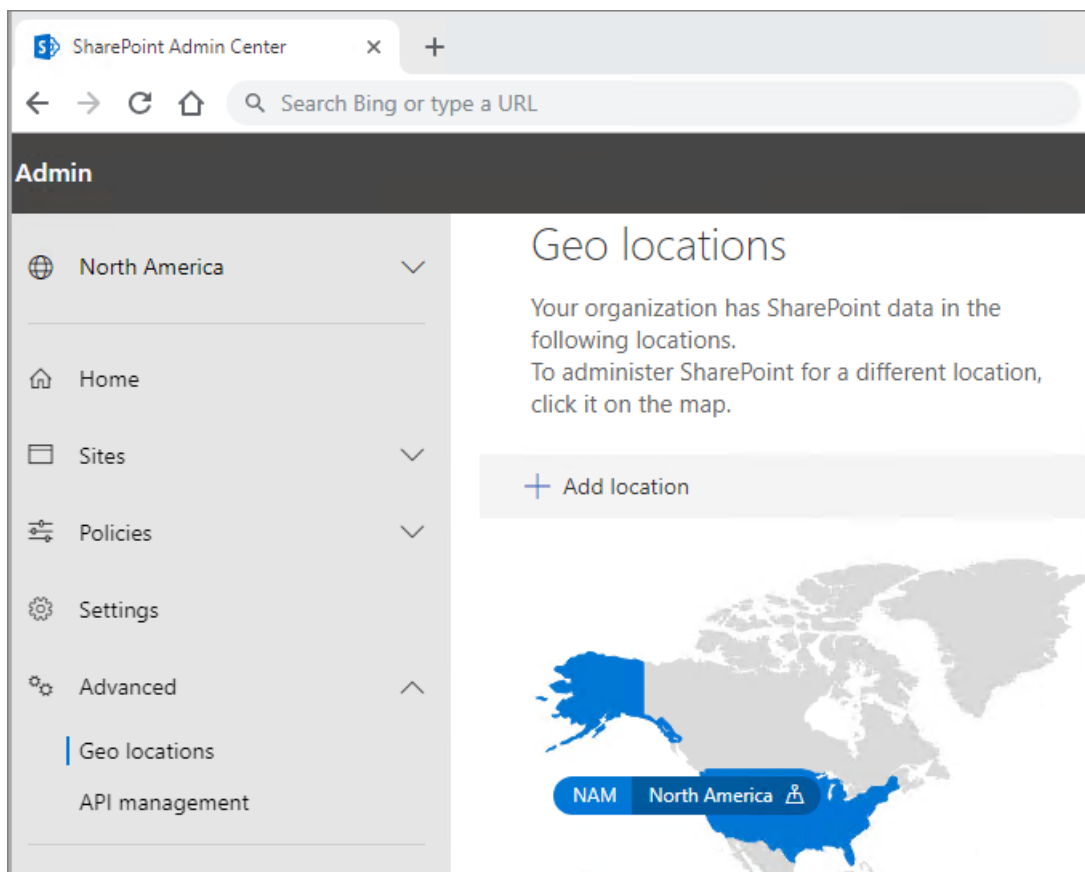
Once your tenant has been provisioned with the *Multi-Geo Capabilities in Microsoft 365* plan, the **Geo locations** tab will become available in the OneDrive and SharePoint admin centers.

Add satellite locations to your tenant

You must add a satellite location for each geo location where you want to store data. Available geo locations are shown in the following table:

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Asia-Pacific	APC	Southeast or East Asia datacenters
Australia	AUS	Southeast or East Asia datacenters
Brazil	BRA	(eDiscovery data location coming soon)
Canada	CAN	US datacenters
Europe / Middle East / Africa	EUR	Europe datacenters
France	FRA	Europe datacenters
Germany	DEU	Europe datacenters
India	IND	Southeast or East Asia datacenters
Japan	JPN	Southeast or East Asia datacenters
Korea	KOR	Southeast or East Asia datacenters
North America	NAM	US datacenters

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Norway	NOR	(eDiscovery data location coming soon)
Qatar	QAT	(eDiscovery data location coming soon)
South Africa	ZAF	Europe datacenters
Sweden	SWE	Europe datacenters
Switzerland	CHE	Europe datacenters
United Arab Emirates	ARE	Southeast or East Asia datacenters
United Kingdom	GBR	Europe datacenters



To add a satellite location

1. Open the SharePoint admin center, and go to [Geo locations](#).
2. Select **Add location**.
3. Select the location that you want to add, and then select **Next**.
4. Type the domain that you want to use with the geo location, and then select **Add**.
5. Select **Close**.

Provisioning may take from a few hours up to 72 hours, depending on the size of your tenant. Once provisioning of a satellite location has completed, you will receive an email confirmation. When the new geo

location appears in blue on the map on the **Geo locations** tab in the OneDrive admin center, you can proceed to set users' preferred data location to that geo location.

IMPORTANT

Your new satellite location will be set up with default settings. This will allow you to configure that satellite location as appropriate for your local compliance needs.

Setting users' preferred data location

Once you enable the needed satellite locations, you can update your user accounts to use the appropriate preferred data location. We recommend that you set a preferred data location for every user, even if that user is staying in the central location.

IMPORTANT

If a user's preferred data location is set to a location that has not been configured as a satellite location or the central location, the system will default to the central location when provisioning OneDrive and SharePoint sites and Group mailboxes.

TIP

We recommend that you begin validations with a test user or small group of users before rolling out multi-geo to your broader organization.

In Azure Active Directory (Azure AD) there are two types of user objects: cloud only users and synchronized users. Please follow the appropriate instructions for your type of user.

Synchronize user's Preferred Data Location using Azure AD Connect

If your company's users are synchronized from an on-premises Active Directory system to Azure AD, their PreferredDataLocation must be populated in AD and synchronized to Azure AD.

Follow the process in [Azure Active Directory Connect sync: Configure preferred data location for Microsoft 365 resources](#) to configure Preferred Data Location sync from your on-premises Active Directory Domain Services (AD DS) to Azure AD.

We recommend that you include setting the user's Preferred Data Location as a part of your standard user creation workflow.

IMPORTANT

For new users with no OneDrive provisioned, license the account and wait at least 48 hours after a user's PDL is synchronized to Azure AD for the changes to propagate before the user logs in to OneDrive for Business. (Setting the preferred data location before the user logs in to provision their OneDrive for Business ensures that the user's new OneDrive will be provisioned in the correct location.)

Setting Preferred Data Location for cloud only users

If your company's users are not synchronized from an on-premises Active Directory system to Azure AD, meaning they are created in Microsoft 365 or Azure AD, then the PDL must be set using the Microsoft Azure Active Directory Module for Windows PowerShell.

The procedures in this section require the [Microsoft Azure Active Directory Module for Windows PowerShell](#)

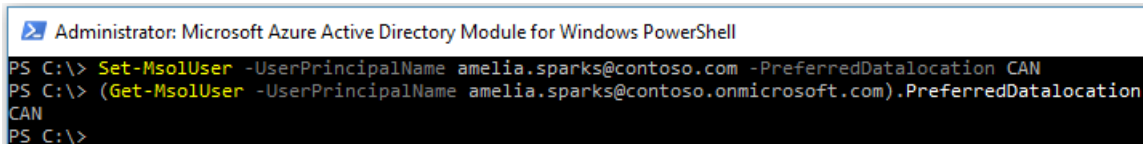
Module. If you already have this module installed, please ensure you update to the latest version.

1. [Connect and sign in](#) with a set of global administrator credentials for your tenant.
2. Use the [Set-MsolUser](#) cmdlet to set the preferred data location for each of your users. For example:

```
Set-MsolUser -UserPrincipalName Robyn.Buckley@Contoso.com -PreferredDataLocation EUR
```

You can check to confirm that the preferred data location was updated properly by using the `Get-MsolUser` cmdlet. For example:

```
(Get-MsolUser -UserPrincipalName Robyn.Buckley@Contoso.com).PreferredDataLocation
```



The screenshot shows a PowerShell terminal window titled "Administrator: Microsoft Azure Active Directory Module for Windows PowerShell". It displays the following commands and output:

```
PS C:\> Set-MsolUser -UserPrincipalName amelia.sparks@contoso.com -PreferredDataLocation CAN
PS C:\> (Get-MsolUser -UserPrincipalName amelia.sparks@contoso.onmicrosoft.com).PreferredDataLocation
CAN
PS C:\>
```

We recommend that you include setting the user's Preferred Data Location as a part of your standard user creation workflow.

IMPORTANT

For new users with no OneDrive provisioned, license the account and wait at least 48 hours after a user's PDL is set for the changes to propagate before the user logs in to OneDrive. (Setting the preferred data location before the user logs in to provision their OneDrive for Business ensures that the user's new OneDrive will be provisioned in the correct location.)

OneDrive Provisioning and the effect of PDL

If the user already has a OneDrive site created in the tenant, setting their PDL will not automatically move their existing OneDrive. To move a user's OneDrive, see [OneDrive for Business Geo Move](#).

NOTE

Exchange Online automatically relocates the user's mailbox if the PDL changes and the MailboxRegion no longer matches the Mailbox Database Geo Location code. For more information, see [Administering Exchange Online mailboxes in a multi-geo environment](#).

If the user does not have a OneDrive site within the tenant, OneDrive will be provisioned for them in accordance to their PDL value, assuming the PDL for the user matches one of the company's satellite locations.

Configuring Multi-Geo search

Your multi-geo tenant will have aggregate search capabilities allowing a search query to return results from anywhere within the tenant.

By default, searches from these entry points will return aggregate results, even though each search index is located within its relevant geo location:

- OneDrive for Business
- Delve
- SharePoint Home
- Search Center

Additionally, multi-geo search capabilities can be configured for your custom search applications that use the SharePoint search API.

Please review [Configure Search for OneDrive for Business Multi-Geo](#) for instructions including any limitations and differences.

Validating the Microsoft 365 Multi-Geo configuration

Below are some basic use cases you may wish to include in your validation plan before broadly rolling out Microsoft 365 Multi-Geo to your company. Once you have completed these tests and any additional use cases that are relevant to your company, you may choose to move on to adding the users in your initial pilot group.

OneDrive for Business:

Select OneDrive from the Microsoft 365 app launcher and confirm that you are automatically directed to the appropriate geo location for the user, based on the user's PDL. OneDrive for Business should now begin provisioning at that location. Once provisioned, try uploading and downloading some documents.

OneDrive Mobile App:

Log in to your OneDrive mobile App with your test account credentials. Confirm that you can see your OneDrive for Business files and can interact with them from your mobile device.

OneDrive sync client:

Confirm that the OneDrive sync client automatically detects your OneDrive for Business geo location upon login. If you need to download the sync client, you can click **Sync** in the OneDrive library.

Office applications:

Confirm that you can access OneDrive for Business by logging in from an Office application, such as Word. Open the Office application and select "OneDrive – <TenantName>". Office will detect your OneDrive location and show you the files that you can open.

Sharing:

Try sharing OneDrive files. Confirm that the people picker shows you all your SharePoint online users regardless of their geo location.

Configure Search for Microsoft 365 Multi-Geo

10/28/2022 • 8 minutes to read • [Edit Online](#)

In a multi-geo environment, each geo location has its own search index and Search Center. When a user searches, the query is fanned out to all the indexes, and the returned results are merged.

For example, a user in one geo location can search for content stored in another geo location, or for content on a SharePoint site that's restricted to a different geo location. If the user has access to this content, search will show the result.

Which search clients work in a multi-geo environment?

These clients can return results from all geo locations:

- OneDrive
- Delve
- The SharePoint home page
- The Search Center
- Custom search applications that use the SharePoint Search API

OneDrive

As soon as the multi-geo environment has been set up, users that search in OneDrive get results from all geo locations.

Delve

As soon as the multi-geo environment has been set up, users that search in Delve get results from all geo locations.

The Delve feed and the profile card only show previews of files that are stored in the central location. For files that are stored in satellite locations, the icon for the file type is shown instead.

The SharePoint home page

As soon as the multi-geo environment has been set up, users will see news, recent and followed sites from multiple geo locations on their SharePoint home page. If they use the search box on the SharePoint home page, they'll get merged results from multiple geo locations.

The Search Center

After the multi-geo environment has been set up, each Search Center continues to only show results from their own geo location. Admins must [change the settings of each Search Center](#) to get results from all geo locations. Afterwards, users that search in the Search Center get results from all geo locations.

Custom search applications

As usual, custom search applications interact with the search indexes by using the existing SharePoint Search REST APIs. To get results from all, or some geo locations, the application must [call the API and include the new Multi-Geo query parameters](#) in the request. This triggers a fan out of the query to all geo locations.

What's different about search in a multi-geo environment?

Some search features you might be familiar with, work differently in a multi-geo environment.

FEATURE	HOW IT WORKS	WORKAROUND
Promoted results	You can create query rules with promoted results at different levels: for the whole tenant, for a site collection, or for a site. In a multi-geo environment, define promoted results at the tenant level to promote the results to the Search Centers in all geo locations. If you only want to promote results in the Search Center that's in the geo location of the site collection or site, define the promoted results at the site collection or site level. These results are not promoted in other geo locations.	If you don't need different promoted results per geo location, for example different rules for traveling, we recommend defining promoted results at the tenant level.
Search refiners	Search returns refiners from all the geo locations of a tenant and then aggregates them. The aggregation is a best effort, meaning that the refiner counts might not be 100% accurate. For most search-driven scenarios, this accuracy is sufficient.	For search-driven applications that depend on refiner completeness, query each geo location independently.
	Multi-geo search doesn't support dynamic bucketing for numerical refiners.	Use the "Discretize" parameter for numerical refiners.
Document IDs	If you're developing a search-driven application that depends on document IDs, note that document IDs in a multi-geo environment aren't unique across geo locations, they are unique per geo location.	We've added a column that identifies the geo location. Use this column to achieve uniqueness. This column is named "GeoLocationSource".
Number of results	The search results page shows combined results from the geo locations, but it's not possible to page beyond 500 results.	
Hybrid search	In a hybrid SharePoint environment with cloud hybrid search , on-premises content is added to the Microsoft 365 index of the central location.	

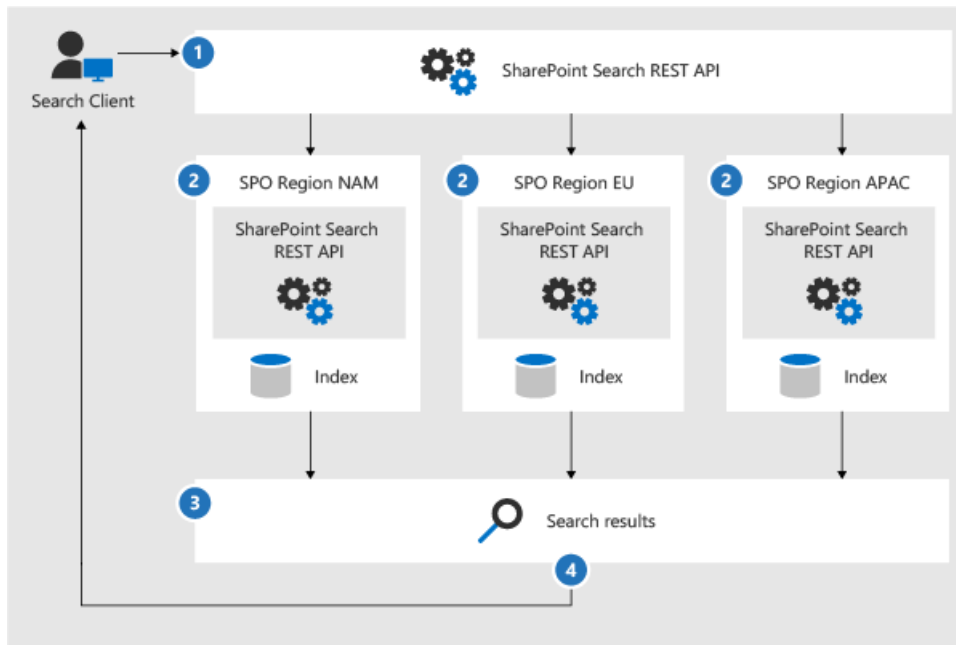
What's not supported for search in a multi-geo environment?

Some of the search features you might be familiar with, aren't supported in a multi-geo environment.

SEARCH FEATURE	NOTE
App-only authentication	App-only authentication (privileged access from services) isn't supported in multi-geo search.
Guests	Guests only get results from the geo location that they're searching from.

How does search work in a multi-geo environment?

All the search clients use the existing SharePoint Search REST APIs to interact with the search indexes.



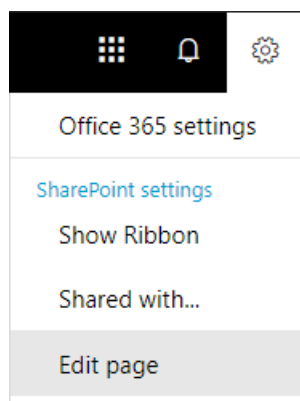
1. A search client calls the Search REST endpoint with the query property `EnableMultiGeoSearch= true`.
2. The query is sent to all geo locations in the tenant.
3. Search results from each geo location are merged and ranked.
4. The client gets unified search results.

Notice that we don't merge the search results until we've received results from all the geo locations. This means that multi-geo searches have additional latency compared to searches in an environment with only one geo location.

Get a Search Center to show results from all geo locations

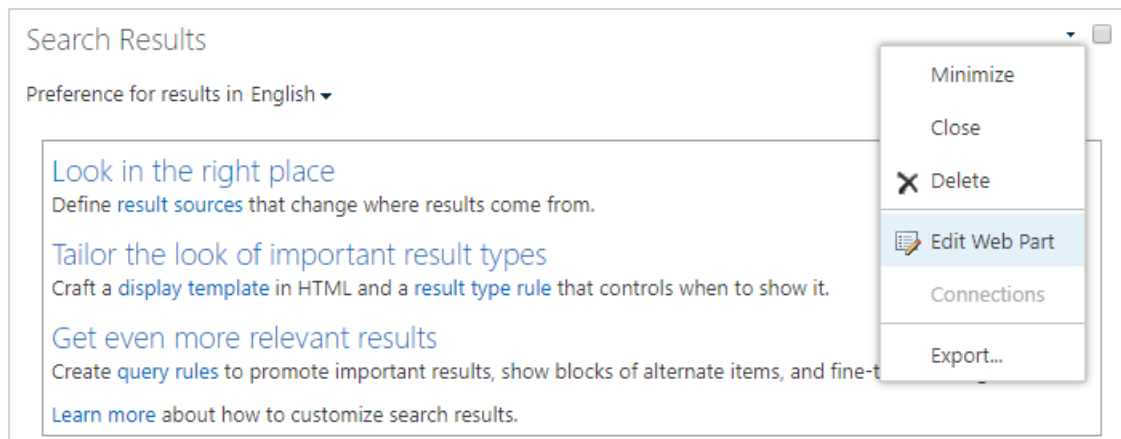
Each Search Center has several verticals and you have to set up each vertical individually.

1. Ensure that you perform these steps with an account that has permission to edit the search results page and the Search Result Web Part.
2. Navigate to the search results page (see the [list](#) of search results pages)
3. Select the vertical to set up, click **Settings** gear icon in the upper, right corner, and then click **Edit Page**. The search results page opens in Edit mode.



4. In the Search Results Web Part, move the pointer to the upper, right corner of the web part, click the

arrow, and then click **Edit Web Part** on the menu. The Search Results Web Part tool pane opens under the ribbon in the top right of the page.



5. In the Web Part tool pane, in the **Settings** section, under **Results control settings**, select **Show Multi-Geo results** to get the Search Results Web Part to show results from all geo locations.
6. Click **OK** to save your change and close the Web Part tool pane.
7. Check your changes to the Search Results Web Part by clicking **Check-In** on the Page tab of the main menu.
8. Publish the changes by using the link provided in the note at the top of the page.

Get custom search applications to show results from all or some geo locations

Custom search applications get results from all, or some, geo locations by specifying query parameters with the request to the SharePoint Search REST API. Depending on the query parameters, the query is fanned out to all geo locations, or to some geo locations. For example, if you only need to query a subset of geo locations to find relevant information, you can control the fan out to only these. If the request succeeds, the SharePoint Search REST API returns response data.

Requirement

For each geo location, you must ensure that all users in the organization have been granted the **Read** permission level for the root website (for example [contosoAPAC.sharepoint.com/](#) and [contosoEU.sharepoint.com/](#)). [Learn about permissions.](#)

Query parameters

EnableMultiGeoSearch - This is a Boolean value that specifies whether the query shall be fanned out to the indexes of other geo locations of the multi-geo tenant. Set it to **true** to fan out the query; **false** to not fan out the query. If you don't include this parameter, the default value is **false**, except when making a REST API call against a site which uses the Enterprise Search Center template, in this case the default value is **true**. If you use the parameter in an environment that isn't multi-geo, the parameter is ignored.

ClientType - This is a string. Enter a unique client name for each search application. If you don't include this parameter, the query is not fanned out to other geo locations.

MultiGeoSearchConfiguration - This is an optional list of which geo locations in the multi-geo tenant to fan the query out to when **EnableMultiGeoSearch** is **true**. If you don't include this parameter, or leave it blank, the query is fanned out to all geo locations. For each geo location, enter the following items, in JSON format:

ITEM	DESCRIPTION
DataLocation	The geo location, for example NAM.
EndPoint	The endpoint to connect to, for example https://contoso.sharepoint.com
SourceId	The GUID of the result source, for example B81EAB55-3140-4312-B0F4-9459D1B4FFEE.

If you omit DataLocation or EndPoint, or if a DataLocation is duplicated, the request fails. [You can get information about the endpoint of a tenant's geo locations by using Microsoft Graph.](#)

Response data

MultiGeoSearchStatus – This is a property that the SharePoint Search API returns in response to a request. The value of the property is a string and gives the following information about the results that the SharePoint Search API returns:

VALUE	DESCRIPTION
Full	Full results from all the geo locations.
Partial	Partial results from one or more geo locations. The results are incomplete due to a transient error.

Query using the REST service

With a GET request, you specify the query parameters in the URL. With a POST request, you pass the query parameters in the body in JavaScript Object Notation (JSON) format.

Request headers

NAME	VALUE
Content-Type	application/json;odata=verbose

Sample GET request that's fanned out to all geo locations

```
https:// \<tenant>\/_api/search/query?
querytext='sharepoint'&Properties='EnableMultiGeoSearch:true'&ClientType='my\_client\_id'
```

Sample GET request to fan out to some geo locations

```
https:// \<tenant>\/_api/search/query?
querytext='site'&ClientType='my_client_id'&Properties='EnableMultiGeoSearch:true,
MultiGeoSearchConfiguration:
[{\DataLocation\\:"NAM"\\,Endpoint\\:"https\\://contosoNAM.sharepoint.com"\\,SourceId\\:"B81EAB55-3140-4312-
B0F4-9459D1B4FFEE"}\\,{\DataLocation\\:"CAN"\\,Endpoint\\:"https\\://contosoCAN.sharepoint-df.com"}]'
```

NOTE

Commas and colons in the list of geo locations for the MultiGeoSearchConfiguration property are preceded by the **backslash** character. This is because GET requests use colons to separate properties and commas to separate arguments of properties. Without the backslash as an escape character, the MultiGeoSearchConfiguration property is interpreted wrongly.

Sample POST request that's fanned out to all geo locations

```
{
  "request": {
    "__metadata": {
      "type": "Microsoft.Office.Server.Search.REST.SearchRequest"
    },
    "Querytext": "sharepoint",
    "Properties": {
      "results": [
        {
          "Name": "EnableMultiGeoSearch",
          "Value": {
            "QueryPropertyValueIndex": 3,
            "BoolVal": true
          }
        }
      ]
    },
    "ClientType": "my_client_id"
  }
}
```

Sample POST request that's fanned out to some geo locations

```
{
  "request": {
    "Querytext": "SharePoint",
    "ClientType": "my_client_id",
    "Properties": {
      "results": [
        {
          "Name": "EnableMultiGeoSearch",
          "Value": {
            "QueryPropertyValueIndex": 3,
            "BoolVal": true
          }
        },
        {
          "Name": "MultiGeoSearchConfiguration",
          "Value": {
            "StrVal": "[{\\"DataLocation\\":\\"NAM\\",\\"Endpoint\\":\\"https://contoso.sharepoint.com\\",\\"SourceId\\":\\"B81EAB55-3140-4312-B0F4-9459D1B4FFEE\\"},{\\"DataLocation\\":\\"CAN\\",\\"Endpoint\\":\\"https://contosoCAN.sharepoint.com\\"}]",
            "QueryPropertyValueIndex": 1
          }
        }
      ]
    }
  }
}
```

Query using CSOM

Here's a sample CSOM query that's fanned out to all geo locations:

```
var keywordQuery = new KeywordQuery(ctx);
keywordQuery.QueryText = query.SearchQueryText;
keywordQuery.ClientType = <enter a string here>;
keywordQuery.Properties["EnableMultiGeoSearch"] = true;
```

Administering a multi-geo environment

10/28/2022 • 4 minutes to read • [Edit Online](#)

Here's a look at how Microsoft 365 services work in a multi-geo environment.

Administrator experience

The SharePoint admin center has a [Geo locations](#) tab in the left navigation that features a geo locations map where you can view and manage your geo locations. Use this page to add or delete geo locations for your tenant.

Audit log search

A unified [Audit log](#) for all your satellite locations is available from the Microsoft 365 audit log search page. You can see all the audit log entries from across geo locations, for example, NAM & EUR users' activities will show up in one org view and then you can apply existing filters to see specific user's activities.

NOTE

Exchange admin audit events are only available for the default location.

BCS, Secure Store, Apps

BCS, Secure Store, and Apps all have separate instances in each satellite location, therefore the SharePoint Online administrator should manage and configure these services separately from each satellite location.

Compliance admin center

There is one central compliance center for a multi-geo tenant: [Microsoft Purview admin center](#).

eDiscovery

By default, an eDiscovery Manager or Administrator of a multi-geo tenant will be able to conduct eDiscovery only in the central location of that tenant. The Office 365 global administrator must assign eDiscovery Manager permissions to allow others to perform eDiscovery and assign a "Region" parameter in their applicable Compliance Security Filter to specify the region for conducting eDiscovery as satellite location, otherwise no eDiscovery will be carried out for the satellite location. To configure the Compliance Security Filter for a Region, see [Configure Office 365 Multi-Geo eDiscovery](#).

Exchange mailboxes

Users' Exchange mailboxes are moved automatically if their PDL is changed. When a new mailbox is created, it is provisioned to the user's PDL or to the central location if no value has been set for the user's PDL.

Information Protection (IP) Data Loss Prevention (DLP) policy

You can set your IP DLP policies for OneDrive for Business, SharePoint, and Exchange in the Security and Compliance center, scoping policies as needed to the whole tenant or to applicable users. For example: If you wish to select a policy for a user in a satellite location, select to apply the policy to a specific OneDrive and enter

the user's OneDrive url. See [Overview of data loss prevention policies](#) for general guidance in creating DLP policies.

The DLP policies are automatically synchronized based on their applicability to each geo location.

Implementing Information Protection and Microsoft Purview Data Loss Prevention policies to all users in a geo location is not an option available in the UI, instead you must select the applicable accounts for the policy or apply the policy globally to all accounts.

Microsoft Power Apps

Power Apps created for the satellite location will use the end point located in the central location for the tenant. Microsoft Power Apps is not a Multi-Geo service.

Power Automate

Flows created for the satellite location will use the end point located in the default geo location for the tenant. Power Automate is not a Multi-Geo service.

SharePoint storage quota

By default, all geo locations of a multi-geo environment share the available tenant storage quota. You can also manage the storage quota by allocating a specific quota for a particular geo location. For more information, see [SharePoint storage quotas in multi-geo environments](#).

Sharing

Administrators can set and manage sharing policies for each of their locations. The OneDrive and SharePoint sites in each geo location will honor only the corresponding geo-specific sharing settings. (For example, you can allow [external sharing](#) for your central location, but not for your satellite location or vice versa.) Note that the sharing settings do not allow configuring sharing limitations between geo locations.

Stream

Videos uploaded to Stream in a 1:1 chat are stored in the OneDrive of the person uploading. Meeting recordings are stored in the OneDrive of each attendee who records the meeting.

Taxonomy

We support a unified [taxonomy](#) for enterprise-managed metadata across geo locations, with the master being hosted in the central location for your company. We recommend that you manage your global taxonomy from the central location and only add location-specific terms to the satellite location's Taxonomy. Global taxonomy terms will synchronize to the satellite locations.

See [Manage metadata in a multi-geo tenant](#) for additional details and for developer guidance.

User Profile Application

There is a [user profile application](#) in each geo location. Each user's profile information is hosted in their geo location and available to the administrator for that geo location.

If you have custom profile properties, then we recommend that you use the same profile schema across geographies and populate your custom profile properties either in all geo locations or where needed. For guidance regarding how to populate user profile data programmatically, please refer to the [Bulk User Profile Update API](#).

See [Work with user profiles in a multi-geo tenant](#) for additional details and for developer guidance.

Yammer

Yammer is not a Multi-Geo workload. Yammer threads stored in Yammer will be placed in the tenant's central location. Yammer is rolling out a file storage change which will store Yammer files within SharePoint. Yammer files stored in SharePoint will be placed the SharePoint site associated with the Yammer group. SharePoint group sites are based on PDL logic as outlined in [SharePoint Sites and Groups](#).

SharePoint storage quotas in multi-geo environments

10/28/2022 • 2 minutes to read • [Edit Online](#)

By default, all geo locations of a multi-geo environment share the available tenant storage quota.

With the SharePoint geo storage quota setting, you can manage the storage quota for each geo location. When you allocate a storage quota for a geo location, it becomes the maximum amount of storage available for that geo location, and is deducted from the available tenant storage quota. The remaining available tenant storage quota is then shared across the configured geo locations for which a specific storage quota has not been allocated.

The SharePoint storage quota for any geo location can be allocated by the SharePoint Online administrator by connecting to the central location. Geo administrators for satellite locations can view the storage quota but cannot allocate it.

Configure a storage quota for a geo location

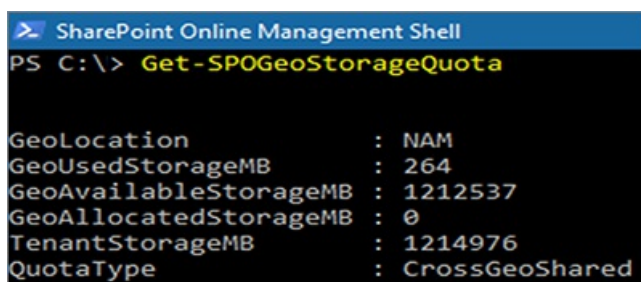
Use the [Microsoft SharePoint Online Module](#) and connect to the central location to allocate the storage quota for a geo location.

To allocate Storage Quota for a location, run cmdlet:

```
Set-SPOGeoStorageQuota -GeoLocation <geolocationcode> -StorageQuotaMB <value>
```

To view Storage Quota for the current geo location, run:

```
Get-SPOGeoStorageQuota
```



```
SharePoint Online Management Shell
PS C:\> Get-SPOGeoStorageQuota

GeoLocation           : NAM
GeoUsedStorageMB      : 264
GeoAvailableStorageMB : 1212537
GeoAllocatedStorageMB : 0
TenantStorageMB       : 1214976
QuotaType              : CrossGeoShared
```

To view Storage Quota for all geo locations, run:

```
Get-SPOGeoStorageQuota -AllLocations
```

To remove the allocated storage quota for a geo location, set `StorageQuota value = 0`:

```
Set-SPOGeoStorageQuota -GeoLocation <geolocationcode> -StorageQuotaMB 0
```

Move a OneDrive site to a different geo location

10/28/2022 • 7 minutes to read • [Edit Online](#)

With OneDrive geo move, you can move a user's OneDrive to a different geo location. OneDrive geo move is performed by the SharePoint Online administrator or the Microsoft 365 global administrator. Before you start a OneDrive geo move, be sure to notify the user whose OneDrive is being moved and recommend they close all files for the duration of the move. (If the user has a document open using the Office client during the move, then upon move completion the document will need to be saved to the new location.) The move can be scheduled for a future time, if desired.

The OneDrive service uses Azure Blob Storage to store content. The Storage blob associated with the user's OneDrive will be moved from the source to destination geo location within 40 days of destination OneDrive being available to the user. The access to the user's OneDrive will be restored as soon as the destination OneDrive is available.

During OneDrive geo move window (about 2-6 hours) the user's OneDrive is set to read-only. The user can still access their files via the OneDrive sync app or their OneDrive site in SharePoint Online. After OneDrive geo move is complete, the user will be automatically connected to their OneDrive at the destination geo location when they navigate to OneDrive in the Microsoft 365 app launcher. The sync app will automatically begin syncing from the new location.

The procedures in this article require the [Microsoft SharePoint Online PowerShell Module](#).

Communicating to your users

When moving OneDrive sites between geo locations, it's important to communicate to your users what to expect. This can help reduce user confusion and calls to your help desk. Email your users before the move and let them know the following information:

- When the move is expected to start and how long it is expected to take
- What geo location their OneDrive is moving to, and the URL to access the new location
- They should close their files and not make edits during the move.
- File permissions and sharing will not change as a result of the move.
- What to expect from the [user experience in a multi-geo environment](#)

Be sure to send your users an email when the move has successfully completed informing them that they can resume working in OneDrive.

Scheduling OneDrive site moves

You can schedule OneDrive site moves in advance (described later in this article). We recommend that you start with a small number of users to validate your workflows and communication strategies. Once you are comfortable with the process, you can schedule moves as follows:

- You can schedule up to 4,000 moves at a time.
- As the moves begin, you can schedule more, with a maximum of 4,000 pending moves in the queue and any given time.
- The maximum size of a OneDrive that can be moved is 1 terabyte (1 TB).

Moving a OneDrive site

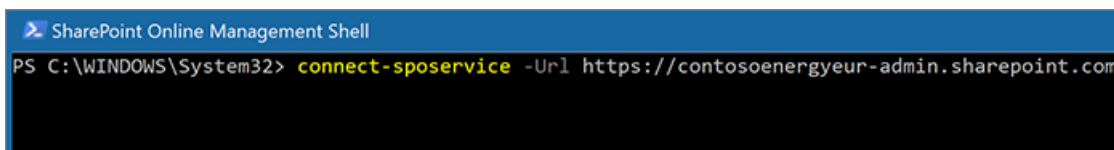
To perform a OneDrive geo move, the tenant administrator must first set the user's Preferred Data Location (PDL) to the appropriate geo location. Once the PDL is set, wait for at least 24 hours for the PDL update to sync across the geo locations before starting the OneDrive geo move.

When using the geo move cmdlets, connect to SPO Service at the user's current OneDrive geo location, using the following syntax:

```
Connect-SPOService -url https://<tenantName>-admin.sharepoint.com
```

For example: To move OneDrive of user 'Matt@contosoenergy.onmicrosoft.com', connect to EUR SharePoint Admin center as the user's OneDrive is in EUR geo location:

```
Connect-SPOService -url https://contosoenergyeur-admin.sharepoint.com
```



Validating the environment

Before you start a OneDrive geo move, we recommend that you validate the environment.

To ensure that all geo locations are compatible, run:

```
Get-SPOGeoMoveCrossCompatibilityStatus
```

This will display all your geo locations and whether the environment is compatible with the destination geo location. If a geo location is incompatible, that means an update is in progress in that location. Try again in a few days.

If a OneDrive contains a subsite, for example, it cannot be moved. You can use the Start-SPOUserAndContentMove cmdlet with the -ValidationOnly parameter to validate if the OneDrive is able to be moved:

```
Start-SPOUserAndContentMove -UserPrincipalName <UPN> -DestinationDataLocation <DestinationDataLocation> -ValidationOnly
```

This will return Success if the OneDrive is ready to be moved or Fail if there is a legal hold or subsite that would prevent the move. Once you have validated that the OneDrive is ready to move, you can start the move.

Start a OneDrive geo move

To start the move, run:

```
Start-SPOUserAndContentMove -UserPrincipalName <UserPrincipalName> -DestinationDataLocation <DestinationDataLocation>
```

Using these parameters:

- *UserPrincipalName* – UPN of the user whose OneDrive is being moved.
- *DestinationDataLocation* – Geo-Location where the OneDrive needs to be moved. This should be same as the user's preferred data location.

For example, to move the OneDrive of matt@contosoenergy.onmicrosoft.com from EUR to AUS, run:

```
Start-SPOUserAndContentMove -UserPrincipalName matt@contosoenergy.onmicrosoft.com -DestinationDataLocation AUS
```

```
> SharePoint Online Management Shell
PS C:\WINDOWS\System32> Start-SPOUserAndContentMove -UserPrincipalName matt@contosoenergy.onmicrosoft.com -DestinationDataLocation AUS
UserPrincipalName      : matt@ContosoEnergy.onmicrosoft.com
SourceDataLocation     : EUR
DestinationDataLocation : AUS
OdbMoveId              : b298219e-3440-10b8-8931-46e805e2b85b
MoveState              : InProgress
```

To schedule a geo move for a later time, use one of the following parameters:

- *PreferredMoveBeginDate* – The move will likely begin at this specified time. Time must be specified in Coordinated Universal Time (UTC).
- *PreferredMoveEndDate* – The move will likely be completed by this specified time, on a best effort basis. Time must be specified in Coordinated Universal Time (UTC).

Cancel a OneDrive geo move

You can stop the geo move of a user's OneDrive, provided the move is not in progress or completed by using the cmdlet:

```
Stop-SPOUserAndContentMove - UserPrincipalName <UserPrincipalName>
```

Where *UserPrincipalName* is the UPN of the user whose OneDrive move you want to stop.

Determining current status

You can check the status of a OneDrive geo move in or out of the geo that you're connected to by using the Get-SPOUserAndContentMoveState cmdlet.

The move statuses are described in the following table.

STATUS	DESCRIPTION
NotStarted	The move has not started
InProgress (n/4)	The move is in progress in one of the following states: • Validation (1/4) • Backup (2/4) • Restore (3/4) • Cleanup (4/4)
Success	The move has completed successfully.
Failed	The move failed.

To find the status of a specific user's move, use the *UserPrincipalName* parameter:

```
Get-SPOUserAndContentMoveState -UserPrincipalName <UPN>
```


To find the status of all of the moves in or out of the geo location that you're connected to, use the *MoveState* parameter with one of the following values: NotStarted, InProgress, Success, Failed, All.

```
Get-SPOUserAndContentMoveState -MoveState <value>
```

You can also add the *Verbose* parameter for more verbose descriptions of the move state.

User Experience

Users of OneDrive should notice minimal disruption if their OneDrive is moved to a different geo location. Aside from a brief read-only state during the move, existing links and permissions will continue to work as expected once the move is completed.

User's OneDrive

While the move is in progress the user's OneDrive is set to read-only. Once the move is completed, the user is directed to their OneDrive in the new geo location when they navigate to OneDrive the Microsoft 365 app launcher or a web browser.

Permissions on OneDrive content

Users with permissions to OneDrive content will continue to have access to the content during the move and after it's complete.

OneDrive sync app

The OneDrive sync app will automatically detect and seamlessly transfer syncing to the new OneDrive location once the OneDrive geo move is complete. The user does not need to sign-in again or take any other action. (Version 17.3.6943.0625 or later of the sync app required.)

If a user updates a file while the OneDrive geo move is in progress, the sync app will notify them that file uploads are pending while the move is underway.

Sharing links

Upon OneDrive geo move completion, the existing shared links for the files that were moved will automatically redirect to the new geo location.

OneNote Experience

OneNote win32 client and UWP (Universal) App will automatically detect and seamlessly sync notebooks to the new OneDrive location once OneDrive geo move is complete. The user does not need to sign-in again or take any other action. The only visible indicator to the user is notebook sync would fail when OneDrive geo move is in progress. This experience is available on the following OneNote client versions:

- OneNote win32 – Version 16.0.8326.2096 (and later)
- OneNote UWP – Version 16.0.8431.1006 (and later)
- OneNote Mobile App – Version 16.0.8431.1011 (and later)

Teams app

Upon OneDrive geo move completion, users will have access to their OneDrive files on the Teams app. Additionally, files shared via Teams chat from their OneDrive prior to geo move will continue to work after move is complete.

OneDrive Mobile App (iOS)

Upon OneDrive geo move completion, the user would need to sign out and sign in again on the iOS Mobile App to sync to the new OneDrive location.

Existing followed groups and sites

Followed sites and groups will show up in the user's OneDrive regardless of their geo location. Sites and groups hosted in another geo location will open in a separate tab.

Delve Geo URL updates

Users will be sent to the Delve geo corresponding to their PDL only after their OneDrive has been moved to the new geo.

Move a SharePoint site to a different geo location

10/28/2022 • 7 minutes to read • [Edit Online](#)

With SharePoint site geo move, you can move SharePoint sites to other geo locations within your multi-geo environment.

The following types of site can be moved between geo locations:

- Microsoft 365 group-connected sites, including those sites associated with Microsoft Teams
- Modern sites without a Microsoft 365 group association
- Classic SharePoint sites
- Communication sites

You must be a Global Administrator or SharePoint Administrator to move a site between geo locations.

There is a read-only window during the SharePoint site geo move of approximately 4-6 hours, depending on site-contents.

Best practices

- Try a SharePoint site move on a test site to get familiar with the procedure.
- Validate whether the site can be moved prior to scheduling or performing the move.
- When possible schedule cross-geo sites moves for outside business hours to reduce user impact.
- Communicate with impacted users prior to the sites move.

Communicating to your users

When moving SharePoint sites between geo locations, it's important to communicate to the sites' users (generally anyone with the ability to edit the site) what to expect. This can help reduce user confusion and calls to your help desk. Email your sites' users before the move and let them know the following information:

- When the move is expected to start and how long it is expected to take
- What geo location their site is moving to, and the URL to access the new location
- They should close their files and not make edits during the move.
- File permissions and sharing will not change because of the move.
- What to expect from the user experience in a multi-geo environment

Be sure to send your sites' users an email when the move has successfully completed informing them that they can resume working on their sites.

Scheduling SharePoint site moves

You can schedule SharePoint site moves in advance (described later in this article). You can schedule moves as follows:

- You can schedule up to 4,000 moves at a time.
- As the moves begin, you can schedule more, with a maximum of 4,000 pending moves in the queue and any given time.
- The maximum size of a SharePoint site that can be moved is 1 terabyte (1 TB).

To schedule a SharePoint site geo move for a later time, include one of the following parameters when you start

the move:

- `PreferredMoveBeginDate` – The move will likely begin at this specified time.
- `PreferredMoveEndDate` – The move will likely be completed by this specified time, on a best effort basis.

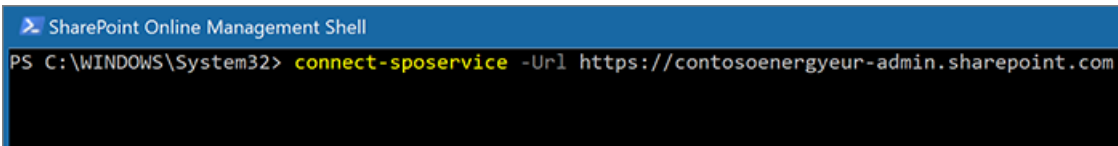
Time must be specified in Coordinated Universal Time (UTC) for both parameters.

Moving the site

SharePoint site geo move requires that you connect and perform the move from the SharePoint Admin URL in the geo location where the site is.

For example, if the site URL is `https://contosohealthcare.sharepoint.com/sites/Turbines`, connect to the SharePoint Admin URL at `https://contosohealthcare-admin.sharepoint.com`:

```
Connect-SPOService -Url https://contosohealthcare-admin.sharepoint.com
```



Validating the environment

We recommend that before scheduling any site move, you perform a validation to ensure that the site can be moved.

We do not support moving sites with:

- Business Connectivity Services
- InfoPath forms
- Information Rights Management (IRM) templates applied

To ensure all geo locations are compatible, run `Get-SPOGeoMoveCrossCompatibilityStatus`. This will display all your geo locations and whether the environment is compatible with the destination geo location. If a geo location is incompatible, that means an update is in progress in that location. Try again in a few days.

To perform a validation-only check on your site, use `Start-SPOSiteContentMove` with the `-ValidationOnly` parameter to validate if the site is able to be moved. For example:

```
Start-SPOSiteContentMove -SourceSiteUrl <SourceSiteUrl> -ValidationOnly -DestinationDataLocation  
<DestinationLocation>
```

This will return *Success* if the site is ready to be moved or *Fail* if any of blocked conditions are present.

Start a SharePoint site geo move for a site with no associated Microsoft 365 group

By default, initial URL for the site will change to the URL of the destination geo location. For example:

```
https://Contoso.sharepoint.com/sites/projectx to https://ContosoEUR.sharepoint.com/sites/projectx
```

For sites with no Microsoft 365 group association, you can also rename the site by using the `-DestinationUrl` parameter. For example:

```
https://Contoso.sharepoint.com/sites/projectx to https://ContosoEUR.sharepoint.com/sites/projecty
```

To start the site move, run:

```
Start-SPOSiteContentMove -SourceSiteUrl <siteURL> -DestinationDataLocation <DestinationDataLocation> -
DestinationUrl <DestinationSiteURL>
```

```
PS C:\WINDOWS\system32> Start-SPOSiteContentMove -DestinationDataLocation EUR
-SourceSiteUrl https://contosohealthcare.sharepoint.com/sites/Turbines

SourceSiteUrl      : https://contosohealthcare.sharepoint.com/sites/Turbines
TargetSiteUrl      : https://contosohealthcareeur.sharepoint.com/sites/Turbines
MoveJobId          : 1f85979e-84d7-707d-2c37-f455d5b6cc94
SourceDataLocation : NAM
DestinationDataLocation : EUR
TimeStamp          : 1/1/0001 00:00:00
MoveState          : InProgress(1/4)
```

Start a SharePoint site geo move for a Microsoft 365 group-connected site

To move a Microsoft 365 group-connected site, the Global Administrator or SharePoint Administrator must first change the Preferred Data Location (PDL) attribute for the Microsoft 365 group.

To set the PDL for a Microsoft 365 group:

```
Set-SPOUnifiedGroup -PreferredDataLocation <PDL> -GroupAlias <GroupAlias>
Get-SPOUnifiedGroup -GroupAlias <GroupAlias>
```

Once you have updated the PDL, you can start the site move:

```
Start-SPOUnifiedGroupMove -GroupAlias <GroupAlias> -DestinationDataLocation <DestinationDataLocation>
```

Cancel a SharePoint site geo move

You can stop a SharePoint site geo move, provided the move is not in progress or completed by using the `Stop-SPOSiteContentMove` cmdlet.

Determining the status of a SharePoint site geo move

You can determine the status of a site move in our out of the geo that you are connected to by using the following cmdlets:

- [Get-SPOSiteContentMoveState](#) (non-Group-connected sites)
- [Get-SPOUnifiedGroupMoveState](#) (Group-connected sites)

Use the `-SourceSiteUrl` parameter to specify the site for which you want to see move status.

The move statuses are described in the following table.

STATUS	DESCRIPTION
Ready to Trigger	The move has not started.
Scheduled	The move is in queue but has not yet started.
InProgress (n/4)	The move is in progress in one of the following states: Validation (1/4), Back up (2/4), Restore (3/4), Cleanup (4/4).
Success	The move has completed successfully.

STATUS	DESCRIPTION
Failed	The move failed.

You can also apply the `-Verbose` option to see additional information about the move.

User experience

Site users should notice minimal disruption when their site is moved to a different geo location. Aside from a brief read-only state during the move, existing links and permissions will continue to work as expected once the move is completed.

Site

While the move is in progress, the site is set to read-only. Once the move is completed, the user is directed to the new site in the new geo location when they click on bookmarks or other links to the site.

Permissions

Users with permissions to site will continue to have access to the site during the move and after it's complete.

Sync app

The sync app will automatically detect and seamlessly transfer syncing to the new site location once the site move is complete. The user does not need to sign in again or take any other action. (Version 17.3.6943.0625 or later of the sync app required.)

If a user updates a file while the move is in progress, the sync app will notify them that file uploads are pending while the move is underway.

Sharing links

When the SharePoint site geo move completes, the existing shared links for the files that were moved will automatically redirect to the new geo location.

Most Recently Used files in Office (MRU)

The MRU service is updated with the site url and its content URLs once the move completes. This applies to Word, Excel, and PowerPoint.

OneNote experience

OneNote win32 client and UWP (Universal) App will automatically detect and seamlessly sync notebooks to the new site location once site move is complete. The user does not need to sign in again or take any other action. The only visible indicator to the user is notebook sync would fail when site move is in progress. This experience is available on the following OneNote client versions:

- OneNote win32 – Version 16.0.8326.2096 (and later)
- OneNote UWP – Version 16.0.8431.1006 (and later)
- OneNote Mobile App – Version 16.0.8431.1011 (and later)

Teams (applicable to Microsoft 365 group connected sites)

When the SharePoint site geo move completes, users will have access to their Microsoft 365 group site files on the Teams app. Additionally, files shared via Teams chat from their site prior to geo move will continue to work after move is complete.

SharePoint site geo move does not support moving Private Channels from one geo to another. Private channels remain in the original geo.

SharePoint Mobile App (iOS/Android)

The SharePoint Mobile App is cross geo compatible and able to detect the site's new geo location.

SharePoint workflows

SharePoint 2013 workflows have to be republished after the site move. SharePoint 2010 workflows should continue to function normally.

Apps

If you are moving a site with apps, you must reinstantiate the app in the site's new geo location as the app and its connections may not be available in the destination geo location.

Power Automate

In most cases, Power Automate Flows will continue to work after a SharePoint site geo move. We recommend that you test them once the move has completed.

Power Apps

Power Apps need to be recreated in the destination location.

Data movement between geo locations

SharePoint uses Azure Blob Storage for its content, while the metadata associated with sites and its files is stored within SharePoint. After the site is moved from its source geo location to its destination geo location, the service will also move its associated Blob Storage. Blob Storage moves complete in approximately 40 days. This will not have any impact to users interaction with the data.

You can check the Blob Storage move status using the [Get-SPOCrossGeoMoveReport](#) cmdlet.

Add or remove a geo administrator in Microsoft 365 Multi-Geo

10/28/2022 • 2 minutes to read • [Edit Online](#)

You can configure separate administrators for each geo location that you have in your tenant. These administrators will have access to the SharePoint Online and OneDrive settings that are specific to their geo location.

Some services - such as the term store - are administered from the central location and replicated to satellite locations. The geo admin for the central location has access to these, whereas geo admins for satellite locations don't.

Global administrators and SharePoint Online administrators continue to have access to settings in the central location and all satellite locations.

Configuring geo administrators

Configuring geo admins requires SharePoint Online PowerShell module.

Use [Connect-SPOService](#) to connect to the admin center of the geo location where you want to add the geo admin. (For example, Connect-SPOService https://ContosoEUR-admin.sharepoint.com.)

To view the existing geo admins of a location, run `Get-SPOGeoAdministrator`

Adding a user as a geo admin

To add a user as a geo admin, run `Add-SPOGeoAdministrator -UserPrincipalName <UPN>`

To remove a user as a Geo Admin of a location, run `Remove-SPOGeoAdministrator -UserPrincipalName <UPN>`

Adding a group as a geo admin

You can add a security group or a mail-enabled security group as a geo admin. (Distribution groups and Microsoft 365 Groups are not supported.)

To add a group as a geo administrator, run `Add-SPOGeoAdministrator -GroupAlias <alias>`

To remove a group as a geo administrator, run `Remove-SPOGeoAdministrator -GroupAlias <alias>`

Note that not all security groups have a group alias. If you want to add a security group that does not have an alias, run [Get-MsolGroup](#) to retrieve a list of groups, find your security group's ObjectID, and then run:

```
Add-SPOGeoAdministrator -ObjectID <ObjectID>
```

To remove a group by using the ObjectID, run `Remove-SPOGeoAdministrator -ObjectID <ObjectID>`

Related topics

[Add-SPOGeoAdministrator](#)

[Get-SPOGeoAdministrator](#)

[Remove-SPOGeoAdministrator](#)

[Set an alias \(MailNickName\) for a security group](#)

Restrict SharePoint site content to a geo location

10/28/2022 • 2 minutes to read • [Edit Online](#)

Under certain circumstances you might choose to enforce a site and its file content to remain in the geo location where the site was created, either by preventing the site from being moved or by preventing the caching of the site's file content in another geo location.

You can do this task by using the [Set-SPOSite](#) cmdlet with the **RestrictedToGeo** parameter. This parameter has a default value of NULL, but you can change it to one of the following restrictions:

RESTRICTION	DESCRIPTION
NoRestriction	The site can be moved to another geo location.
BlockMoveOnly	Site cannot be moved to another geo location, but site content can be cached in other geo locations.
BlockFull	Site cannot be moved to another geo location, and full file content is not cached in other geo locations. Files' title (harvested from the content), file name, and other properties of the file can still be cached in other geo-locations. Content stored in the site before it was configured to BlockFull, may continue to be cached in other geo locations.

Use the following syntax:

```
Set-SPOSite -Identity <siteURL> -RestrictedToGeo <restriction>
```

For example:

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/RegionRestrictedTeamSite -RestrictedToGeo  
BlockFull
```

Microsoft 365 Multi-Geo eDiscovery configuration

10/28/2022 • 2 minutes to read • [Edit Online](#)

[eDiscovery \(Premium\) capabilities](#) allow a multi-geo eDiscovery administrator to search all of the geos without needing to utilize a "Region" security filter. Data is exported to the Azure instance of the central location of the multi-geo tenant.

Without eDiscovery (Premium) capabilities, an eDiscovery manager or administrator of a multi-geo tenant will be able to conduct eDiscovery only in the central location of that tenant. To support the ability to conduct eDiscovery for satellite locations, a new compliance security filter parameter named "Region" is available via PowerShell. This parameter can be used by tenants whose central location is in North America, Europe, or Asia Pacific. eDiscovery (Premium) is recommended for tenants whose central location is not in North America, Europe, or Asia Pacific and who need to perform eDiscovery across satellite geo locations.

The Microsoft 365 global administrator must assign eDiscovery Manager permissions to allow others to perform eDiscovery and assign a "Region" parameter in their applicable Compliance Security Filter to specify the region for conducting eDiscovery as satellite location, otherwise, no eDiscovery will be carried out for the satellite location. Only one "Region" security filter per user is supported.

When the eDiscovery Manager or Administrator role is set for a particular satellite location, the eDiscovery Manager or Administrator will only be able to perform eDiscovery search actions against the SharePoint sites and OneDrive sites located in that satellite location. If an eDiscovery Manager or Administrator attempts to search SharePoint or OneDrive sites outside the specified satellite location, no results will be returned. Also, when the eDiscovery Manager or Administrator for a satellite location triggers an export, data is exported to the Azure instance of that region. This helps organizations stay in compliance by not allowing content to be exported across controlled borders.

NOTE

If it's necessary for an eDiscovery Manager to search across multiple SharePoint satellite locations, another user account will need to be created for the eDiscovery Manager which specifies the alternate satellite location where the OneDrive or SharePoint sites are located.

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Asia-Pacific	APC	Southeast or East Asia datacenters
Australia	AUS	Southeast or East Asia datacenters
Brazil	BRA	(eDiscovery data location coming soon)
Canada	CAN	US datacenters
Europe / Middle East / Africa	EUR	Europe datacenters
France	FRA	Europe datacenters
Germany	DEU	Europe datacenters

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
India	IND	Southeast or East Asia datacenters
Japan	JPN	Southeast or East Asia datacenters
Korea	KOR	Southeast or East Asia datacenters
North America	NAM	US datacenters
Norway	NOR	(eDiscovery data location coming soon)
Qatar	QAT	(eDiscovery data location coming soon)
South Africa	ZAF	Europe datacenters
Sweden	SWE	Europe datacenters
Switzerland	CHE	Europe datacenters
United Arab Emirates	ARE	Southeast or East Asia datacenters
United Kingdom	GBR	Europe datacenters

To set the Compliance Security Filter for a Region:

1. [Connect to Microsoft 365 Security & Compliance PowerShell](#)
2. Use the following syntax:

```
New-ComplianceSecurityFilter -Action All -FilterName <TheNameYouWantToAssign> -Region <RegionValue> -Users <UserPrincipalName>
```

For example:

```
New-ComplianceSecurityFilter -Action All -FilterName "NAM eDiscovery Managers" -Region NAM -Users adwood@contoso.onmicrosoft.com
```

See the [New-ComplianceSecurityFilter](#) article for additional parameters and syntax.

Create a Microsoft 365 group with a specific preferred data location

10/28/2022 • 2 minutes to read • [Edit Online](#)

When users in a multi-geo environment create a Microsoft 365 group, the group preferred data location (PDL) is automatically set to that of the user. Global, SharePoint, and Exchange Administrators can create groups in any region they select.

If you need to create a group with a specific PDL, you can do that using from the [SharePoint admin center](#) or through the Exchange Online New-UnifiedGroup Microsoft PowerShell cmdlet. When you do this, both the group mailbox and SharePoint site associated with the group will be provisioned in the specified PDL.

To create a Microsoft 365 group with the PDL that you specify, go to the [SharePoint admin center](#) in the geo location where you want to create the group site.

For example:

If you want to create a group site in your Australia location, you can go to

```
https://ContosoAUS-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement
```

1. Select + **Create**.
2. Follow the process to create a group site.

Your group site will be provisioned in the geo location corresponding to the SharePoint admin center from which you initiated the site creation request.

Using Exchange PowerShell

Connect to Exchange Online PowerShell and pass the parameter *-MailBoxRegion* with the geo location code.

For example:

```
New-UnifiedGroup -DisplayName MultiGeoEUR -Alias "MultiGeoEUR" -AccessType Public -MailboxRegion EUR
```

```
PS C:\> New-UnifiedGroup -DisplayName MultiGeoEUR -Alias "MultiGeoEUR" -AccessType Public -MailboxRegion EUR
Name                                     DisplayName GroupType PrimarySmtAddress
-----
MultiGeoEUR_675508cb-5c1b-4523-bc26-2ddb740b04d3 MultiGeoEUR Universal MultiGeoEUR@ContosoEnterprise.onmicrosoft.com
```

NOTE

SharePoint group site provisioning is on-demand. The site will be provisioned the first time a group owner or member attempts to access it.

Geo location codes

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Asia-Pacific	APC	Southeast or East Asia datacenters
Australia	AUS	Southeast or East Asia datacenters

GEO LOCATION	CODE	EDISCOVERY DATA LOCATION
Brazil	BRA	(eDiscovery data location coming soon)
Canada	CAN	US datacenters
Europe / Middle East / Africa	EUR	Europe datacenters
France	FRA	Europe datacenters
Germany	DEU	Europe datacenters
India	IND	Southeast or East Asia datacenters
Japan	JPN	Southeast or East Asia datacenters
Korea	KOR	Southeast or East Asia datacenters
North America	NAM	US datacenters
Norway	NOR	(eDiscovery data location coming soon)
Qatar	QAT	(eDiscovery data location coming soon)
South Africa	ZAF	Europe datacenters
Sweden	SWE	Europe datacenters
Switzerland	CHE	Europe datacenters
United Arab Emirates	ARE	Southeast or East Asia datacenters
United Kingdom	GBR	Europe datacenters

Related topics

[Connect to Exchange Online PowerShell](#)

[Create groups with a specific preferred data location using Graph API](#)

Delete a satellite location in Microsoft 365 Multi-Geo

10/28/2022 • 2 minutes to read • [Edit Online](#)

If you no longer need a satellite location, you can delete it from your tenant from the [SharePoint admin center](#).

WARNING

All user data in the satellite location will be permanently deleted. This includes all OneDrive for Business content, SharePoint sites and Exchange mailboxes including Microsoft 365 Group mailboxes. You must migrate any data to another satellite location or the central location before you delete the satellite location. This action cannot be undone.

Only global administrators can delete satellite locations.

The screenshot shows the 'Geo locations' page in the SharePoint admin center. On the left, there's a map of North America with a 'Delete location (EUR)' button. The main panel is titled 'Delete satellite location' and contains the following content:

If you delete this location, you won't be able to restore it. All the data will be permanently deleted. [Learn more](#)

Delete all data in geo location EMEA:

SharePoint sites	47
OneDrive sites	12

Yes, I acknowledge that I am responsible for duplicating or migrating the data before deleting this satellite location. ☒

Yes, I want to permanently delete this satellite location and all its data. ☒

At the bottom, there are 'Delete' and 'Cancel' buttons.

To delete a satellite location

1. Open the SharePoint admin center, and go to the [Geo locations tab](#).
2. On the map, select the geo location that you want to delete.
3. Select **Delete location**.
4. Confirm the deletion by selecting the confirmation check boxes.
5. Select **Delete**.

Enabling SharePoint Multi-Geo in your satellite geo location

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article is for Global or SharePoint administrators who have created a Multi-Geo satellite location **before** SharePoint Multi-Geo capabilities became generally available on March 27, 2019, and who have not enabled SharePoint Multi-Geo in their satellite geo location(s).

NOTE

If you have added a new geo location **after March 27th, 2019**, you do not need to perform these instructions, as your new geo location will already be enabled for OneDrive and SharePoint Multi-Geo.

These instructions will allow you to enable SharePoint in your satellite location, so your Multi-Geo satellite users can take advantage of both OneDrive and SharePoint Multi-Geo capabilities in O365.

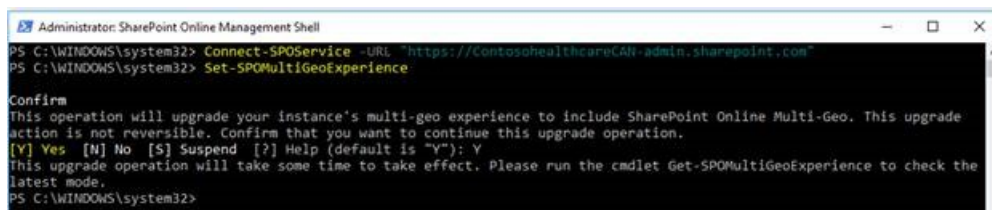
IMPORTANT

Please note that this is a one way enablement. Once you set SPO mode, you will not be able to revert your tenant to OneDrive only Multi-Geo mode without an escalation with support.

To set a geo location into SPO Mode

To set a geo location into SPO mode, connect to the geo location you want to set in SPO Mode:

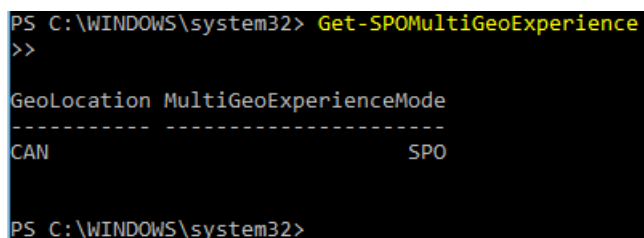
1. Open your SharePoint Online Management Shell
2. Connect-SPOService -URL "https://\$tenantGeo-admin.sharepoint.com" -Credential \$credential
3. Set-SPOMultiGeoExperience



```
Administrator: SharePoint Online Management Shell
PS C:\WINDOWS\system32> Connect-SPOService -URL "https://ContosoHealthcareCAN-admin.sharepoint.com"
PS C:\WINDOWS\system32> Set-SPOMultiGeoExperience

Confirm
This operation will upgrade your instance's multi-geo experience to include SharePoint Online Multi-Geo. This upgrade
action is not reversible. Confirm that you want to continue this upgrade operation.
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
This upgrade operation will take some time to take effect. Please run the cmdlet Get-SPOMultiGeoExperience to check the
latest mode.
PS C:\WINDOWS\system32>
```

4. This operation usually takes about an hour while we perform various publish backs in the service and re-stamp your tenant. After at least 1 hour, please perform a Get-SPOMultiGeoExperience. This will show you whether this geo location is in SPO mode.



```
PS C:\WINDOWS\system32> Get-SPOMultiGeoExperience
>>

GeoLocation MultiGeoExperienceMode
-----
CAN SPO

PS C:\WINDOWS\system32>
```

NOTE

Certain caches in the service update every 24 hours, so it is possible that for a period of up to 24 hours, your satellite geo may intermittently behave as if it was still in ODB mode. This does not cause any technical issues.

For additional information regarding SharePoint Multi-Geo, please refer to aka.ms/sharepointmultigeo

Administering Exchange Online mailboxes in a multi-geo environment

10/28/2022 • 9 minutes to read • [Edit Online](#)

Exchange Online PowerShell is required to view and configure multi geo properties in your Microsoft 365 environment. To connect to Exchange Online PowerShell, see [Connect to Exchange Online PowerShell](#).

You need the [Microsoft Azure Active Directory PowerShell Module](#) v1.1.166.0 or later in v1.x to see the **PreferredDataLocation** property on user objects. User objects synchronized via AAD Connect into AAD cannot have their **PreferredDataLocation** value directly modified via AAD PowerShell. Cloud-only user objects can be modified via AAD PowerShell. To connect to Azure AD PowerShell, see [Connect to PowerShell](#).

In Exchange Online multi-geo environments, you don't need to do any manual steps to add geos to your tenant. After you receive the Message Center post that says multi-geo is ready for Exchange Online, all available geos will be ready and configured for you to use.

Connect directly to a geo location using Exchange Online PowerShell

Typically, Exchange Online PowerShell will connect to the central geo location. But, you can also connect directly to satellite geo locations. Because of performance improvements, we recommend connecting directly to the satellite geo location when you only manage users in that location.

The requirements for installing and using the Exchange Online PowerShell module are described in [Install and maintain the Exchange Online PowerShell module](#).

To connect Exchange Online PowerShell to a specific geo location, the *ConnectionUri* parameter is different than the regular connection instructions. The rest of the commands and values are the same.

Specifically, you need to add the `?email=<emailaddress>` value to end of the *ConnectionUri* value.

`<emailaddress>` is the email address of **any** mailbox in the target geo location. Your permissions to that mailbox or the relationship to your credentials are not a factor; the email address simply tells Exchange Online PowerShell where to connect.

Microsoft 365 or Microsoft 365 GCC customers typically don't need to use the *ConnectionUri* parameter to connect to Exchange Online PowerShell. But, to connect to a specific geo location, you do need to use *ConnectionUri* parameter so you can use `?email=<emailaddress>` in the value.

Connect to a geo location in Exchange Online PowerShell

The following connection instructions work for accounts that are or aren't configured for multi-factor authentication (MFA).

1. In a PowerShell window, load the Exchange Online PowerShell module by running the following command:

```
Import-Module ExchangeOnlineManagement
```

2. In the following example, admin@contoso.onmicrosoft.com is the admin account, and the target geo location is where the mailbox olga@contoso.onmicrosoft.com resides.

```
Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com -ConnectionUri  
https://outlook.office365.com/powershell?email=olga@contoso.onmicrosoft.com
```

3. Enter the password for the admin@contoso.onmicrosoft.com in the prompt that appears. If the account is configured for MFA, you also need to enter the security code.

View the available geo locations that are configured in your Exchange Online organization

To see the list of configured geo locations in Microsoft 365 Multi-Geo, run the following command in Exchange Online PowerShell:

```
Get-OrganizationConfig | Select -ExpandProperty AllowedMailboxRegions | Format-Table
```

View the central geo location for your Exchange Online organization

To view your tenant's central geo location, run the following command in Exchange Online PowerShell:

```
Get-OrganizationConfig | Select DefaultMailboxRegion
```

Find the geo location of a mailbox

The **Get-Mailbox** cmdlet in Exchange Online PowerShell displays the following multi-geo related properties on mailboxes:

- **Database:** The first 3 letters of the database name correspond to the geo code, which tells you where the mailbox is currently located. For Online Archive Mailboxes the **ArchiveDatabase** property should be used.
- **MailboxRegion:** Specifies the geo location code that was set by the admin (synchronized from **PreferredDataLocation** in Azure AD).
- **MailboxRegionLastUpdateTime:** Indicates when MailboxRegion was last updated (either automatically or manually).

To see these properties for a mailbox, use the following syntax:

```
Get-Mailbox -Identity <MailboxIdentity> | Format-List Database,MailboxRegion*
```

For example, to see the geo location information for the mailbox chris@contoso.onmicrosoft.com, run the following command:

```
Get-Mailbox -Identity chris@contoso.onmicrosoft.com | Format-List Database, MailboxRegion*
```

The output of the command looks like this:

```
Database           : EURPR03DG077-db007  
MailboxRegion      : EUR  
MailboxRegionLastUpdateTime : 2/6/2018 8:21:01 PM
```

NOTE

If the geo location code in the database name doesn't match **MailboxRegion** value, the mailbox will be automatically be put into a relocation queue and moved to the geo location specified by the **MailboxRegion** value (Exchange Online looks for a mismatch between these property values).

Move an existing cloud-only mailbox to a specific geo location

A cloud-only user is a user not synchronized to the tenant via AAD Connect. This user was created directly in Azure AD. Use the **Get-MsolUser** and **Set-MsolUser** cmdlets in the Azure AD Module for Windows PowerShell to view or specify the geo location where a cloud-only user's mailbox will be stored.

To view the **PreferredDataLocation** value for a user, use this syntax in Azure AD PowerShell:

```
Get-MsolUser -UserPrincipalName <UserPrincipalName> | Format-List UserPrincipalName,PreferredDataLocation
```

For example, to see the **PreferredDataLocation** value for the user michelle@contoso.onmicrosoft.com, run the following command:

```
Get-MsolUser -UserPrincipalName michelle@contoso.onmicrosoft.com | Format-List
```

To modify the **PreferredDataLocation** value for a cloud-only user object, use the following syntax in Azure AD PowerShell:

```
Set-MsolUser -UserPrincipalName <UserPrincipalName> -PreferredDataLocation <GeoLocationCode>
```

For example, to set the **PreferredDataLocation** value to the European Union (EUR) geo for the user michelle@contoso.onmicrosoft.com, run the following command:

```
Set-MsolUser -UserPrincipalName michelle@contoso.onmicrosoft.com -PreferredDataLocation EUR
```

NOTE

- As mentioned previously, you cannot use this procedure for synchronized user objects from on-premises Active Directory. You need to change the **PreferredDataLocation** value in Active Directory and synchronize it using AAD Connect. For more information, see [Azure Active Directory Connect sync: Configure preferred data location for Microsoft 365 resources](#).
- How long it takes to relocate a mailbox to a new geo location depends on several factors:
 - The size and type of mailbox.
 - The number of mailboxes being moved.
 - The availability of move resources.

Move an inactive mailbox to a specific geo

You can't move inactive mailboxes that are preserved for compliance purposes (for example, mailboxes on Litigation Hold) by changing their **PreferredDataLocation** value. To move an inactive mailbox to a different geo, do the following steps:

- Recover the inactive mailbox. For instructions, see [Recover an inactive mailbox](#).
- Prevent the Managed Folder Assistant from processing the recovered mailbox by replacing

<MailboxIdentity> with the name, alias, account, or email address of the mailbox and running the following command in [Exchange Online PowerShell](#):

```
Set-Mailbox <MailboxIdentity> -ElcProcessingDisabled $true
```

3. Assign an **Exchange Online Plan 2** license to the recovered mailbox. This step is required to place the mailbox back on Litigation Hold. For instructions, see [Assign licenses to users](#).
4. Configure the **PreferredDataLocation** value on the mailbox as described in the previous section.
5. After you've confirmed that the mailbox has moved to the new geo location, place the recovered mailbox back on Litigation Hold. For instructions, see [Place a mailbox on Litigation Hold](#).
6. After verifying that the Litigation Hold is in place, allow the Managed Folder Assistant to process the mailbox again by replacing <MailboxIdentity> with the name, alias, account, or email address of the mailbox and running the following command in [Exchange Online PowerShell](#):

```
Set-Mailbox <MailboxIdentity> -ElcProcessingDisabled $false
```

7. Make the mailbox inactive again by removing the user account that's associated with the mailbox. For instructions, see [Delete a user from your organization](#). This step also releases the Exchange Online Plan 2 license for other uses.

Note: When you move an inactive mailbox to a different geo location, you might affect content search results or the ability to search the mailbox from the former geo location. For more information, see [Searching and exporting content in Multi-Geo environments](#).

Create new cloud mailboxes in a specific geo location

To create a new mailbox in a specific geo location, you need to do either of these steps:

- Configure the **PreferredDataLocation** value as described in the previous [Move an existing cloud-only mailbox to a specific geo location](#) section *before* you create the mailbox in Exchange Online. For example, configure the **PreferredDataLocation** value on a user before you assign a license.
- Assign a license at the same time you set the **PreferredDataLocation** value.

To create a new cloud-only licensed user (not AAD Connect synchronized) in a specific geo location, use the following syntax in Azure AD PowerShell:

```
New-MsolUser -UserPrincipalName <UserPrincipalName> -DisplayName "<Display Name>" [-FirstName <FirstName>]  
[-LastName <LastName>] [-Password <Password>] [-LicenseAssignment <AccountSkuId>] -PreferredDataLocation  
<GeoLocationCode>
```

This example create a new user account for Elizabeth Brunner with the following values:

- User principal name: ebrunner@contoso.onmicrosoft.com
- First name: Elizabeth
- Last name: Brunner
- Display name: Elizabeth Brunner
- Password: randomly-generated and shown in the results of the command (because we're not using the *Password* parameter)
- License: `contoso:ENTERPRISEPREMIUM` (E5)
- Location: Australia (AUS)

```
New-MsolUser -UserPrincipalName ebrunner@contoso.onmicrosoft.com -DisplayName "Elizabeth Brunner" -FirstName Elizabeth -LastName Brunner -LicenseAssignment contoso:ENTERPRISEPREMIUM -PreferredDataLocation AUS
```

For more information about creating new user accounts and finding LicenseAssignment values in Azure AD PowerShell, see [Create user accounts with PowerShell](#) and [View licenses and services with PowerShell](#).

NOTE

If you are using Exchange Online PowerShell to enable a mailbox and need the mailbox to be created directly in the geo location that's specified in **PreferredDataLocation**, you need to use an Exchange Online cmdlet such as **Enable-Mailbox** or **New-Mailbox** directly against the cloud service. If you use the **Enable-RemoteMailbox** cmdlet in on-premises Exchange PowerShell, the mailbox will be created in the central geo location.

Onboard existing on-premises mailboxes in a specific geo location

You can use the standard onboarding tools and processes to migrate a mailbox from an on-premises Exchange organization to Exchange Online, including the [Migration dashboard in the EAC](#), and the [New-MigrationBatch](#) cmdlet in Exchange Online PowerShell.

The first step is to verify a user object exists for each mailbox to be onboarded, and verify the correct **PreferredDataLocation** value is configured in Azure AD. The onboarding tools will respect the **PreferredDataLocation** value and will migrate the mailboxes directly to the specified geo location.

Or, you can use the following steps to onboard mailboxes directly in a specific geo location using the [New-MoveRequest](#) cmdlet in Exchange Online PowerShell.

1. Verify the user object exists for each mailbox to be onboarded and that **PreferredDataLocation** is set to the desired value in Azure AD. The value of **PreferredDataLocation** will be synchronized to the **MailboxRegion** attribute of the corresponding mail user object in Exchange Online.
2. Connect directly to the specific satellite geo location using the connection instructions from earlier in this topic.
3. In Exchange Online PowerShell, store the on-premises administrator credentials that's used to perform a mailbox migration in a variable by running the following command:

```
$RC = Get-Credential
```

4. In Exchange Online PowerShell, create a new **New-MoveRequest** similar to the following example:

```
New-MoveRequest -Remote -RemoteHostName mail.contoso.com -RemoteCredential $RC -Identity user@contoso.com -TargetDeliveryDomain <YourAppropriateDomain>
```

5. Repeat step #4 for every mailbox you need to migrate from on-premises Exchange to the satellite geo location you are currently connected to.
6. If you need to migrate additional mailboxes to different satellite geo locations, repeat steps 2 through 4 for each specific location.

Multi-geo reporting

NOTE

The multi-geo reporting feature is currently in Preview, is not available in all organizations, and is subject to change.

Multi-Geo Usage Reports in the Microsoft 365 admin center displays the user count by geo location. The report displays user distribution for the current month and provides historical data for the past 6 months.

See also

[Manage Microsoft 365 with PowerShell](#)

Moving core data to new Microsoft 365 datacenter geos

10/28/2022 • 3 minutes to read • [Edit Online](#)

We continue to open new datacenter geos for Microsoft 365 services. These new datacenter geos add capacity and compute resources to support our ongoing customer demand and usage growth. Additionally, the new datacenter geos offer in-geo data residency for core customer data.

Core customer data is a term that refers to a subset of customer data including:

- Exchange Online mailbox content (email body, calendar entries, and the content of email attachments)
- SharePoint Online site content and the files stored within that site
- Files uploaded to OneDrive for Business
- Teams chat messages, including private messages, channel messages, and images used in chats

Existing customers that have their core customer data stored in an already existing datacenter geo are not impacted by the launch of a new datacenter geo. We introduce no unique capabilities, features or compliance certifications with the new datacenter geo. As a customer in any of those two geos, you will experience the same quality of service, performance and security controls as you did before. We offer existing customers listed in the table below an option to request early migration of their organization's core customer data at rest to their new datacenter geo.

CUSTOMERS WITH TENANT SIGNUP COUNTRY IN	PREVIOUS DATACENTER GEO	NEW DATACENTER GEO	GEO AVAILABLE SINCE
Japan	Asia/Pacific	Japan	December 2014
Australia, New Zealand, Fiji	Asia/Pacific	Australia	March 2015
India	Asia/Pacific	India	October 2015
Canada	United States	Canada	May 2016
United Kingdom	European Union	United Kingdom	September 2016
South Korea	Asia/Pacific	South Korea	April 2017
France	European Union	France	March 2018
United Arab Emirates	European Union	United Arab Emirates	June 2019
South Africa	European Union	South Africa	July 2019
Switzerland, Liechtenstein	European Union	Switzerland	December 2019
Germany	European Union	Germany	December 2019

CUSTOMERS WITH TENANT SIGNUP COUNTRY IN	PREVIOUS DATACENTER GEO	NEW DATACENTER GEO	GEO AVAILABLE SINCE
Norway	European Union	Norway	April 2020
Brazil	Americas	Brazil	November 2020
Sweden	European Union	Sweden	November 2021
Qatar	European Union	Qatar	August 2022

As of October 1, 2020 customers with an Office 365 Education subscription included in the tenant are not eligible for migration.

A complete list of all datacenter geos, datacenters, and the location of customer data at rest is available as part of the [interactive datacenter maps](#).

Data residency option

We provide a data residency option to eligible Microsoft 365 customers who are covered by the datacenter geos listed in the table above. With this option, eligible customers with data residency requirements can request migration of their organization's core customer data at rest to their new datacenter geo. Microsoft will offer a committed deadline to all eligible customers who request migration during the enrollment window. Review the [How to request your data move](#) page for more details about the open enrollment window for your datacenter geo and the steps to enroll into the program. Data moves can take up to 24 months after the request period ends to complete.

We introduce no unique capabilities, features or compliance certifications with the new datacenter geo.

The complexity, precision and scale at which we need to perform data moves within a globally operated and automated environment prohibit us from sharing when a data move is expected to complete for your tenant or any other single tenant. Customers will receive one confirmation in Message Center per participating service when its data move has completed.

Data moves are a back-end service operation with minimal impact to end-users. Features that can be impacted are listed on the [During and after your data move](#) page. We adhere to the [Microsoft Online Services Service Level Agreement \(SLA\)](#) for availability so there is nothing that customers need to prepare for or to monitor during the move. Notification of any service maintenance is done if needed.

Data moves to the new datacenter geo are completed at no additional cost to the customer.

During the migration process, Microsoft temporarily copies your address book data into Microsoft global resources where it is encrypted and only used to support business continuity and disaster recovery operations (BCDR). After Microsoft has completed the mailbox data moves, Microsoft deletes that temporary data from the global resources. Microsoft continues to invest in global and regional resources on a regular basis. In calendar year 2023, Microsoft plans to utilize regional resources for BCDR purposes during the migration process.

Related topics

[How to request your data move](#)

[Data move general FAQ](#)

[New datacenter geos for Microsoft Dynamics CRM Online](#)

[Azure services by region](#)

How to request your data move

10/28/2022 • 2 minutes to read • [Edit Online](#)

NOTE

The information on this page only applies to customers who had existing Microsoft 365 tenants before the new datacenters in their datacenter geo opened. Migration eligibility also depends on the specific service provisioning date. The tenant creation date may not always be the single date that matters.

Eligible Microsoft 365 customers may request migration for their entire organization's core customer data at rest. The program supports requests for each country in the time period described in the table and from customers with an eligible signup country associated with their Microsoft 365 tenant.

When can I request a move?

CUSTOMERS WITH SIGNUP COUNTRY IN	REQUEST PERIOD BEGINS	REQUEST DEADLINE
Japan		Request period closed
Australia, New Zealand, Fiji		Request period closed
India		Request period closed
Canada		Request period closed
United Kingdom		Request period closed
South Korea		Request period closed
France		Request period closed
United Arab Emirates		Request period closed
South Africa		Request period closed
Switzerland, Liechtenstein		Request period closed
Norway		Request period closed
Germany		Request period closed
Brazil		Request period closed
Sweden		Request period closed
Qatar	August 30, 2022	February 28, 2023

How to request a move

Eligible customers will see a page in the Microsoft 365 admin center, which will allow them to request to have their core customer data moved to their new datacenter region.

To access the page in the Microsoft 365 admin center, in the navigation pane on the left, expand **Settings**, and then click **Org Settings**. Select the tab **Organization profile**, then select the option **Data residency**.

You will not see this section if your tenant is not eligible for the Microsoft 365 Move Program. If your organization has data residency requirements and you need to request migration, mark the checkbox and then **Save**.

Data residency

Data residency is where your organization's core customer data at rest is stored. Core customer data is a term that refers to a subset of customer data including:

- Exchange mailbox content (email body, calendar entries, and the content of email attachments)
- SharePoint site content and the files stored within that site
- Files uploaded to OneDrive for Business
- Teams chat messages, including private messages, channel messages, and images used in chats

No action is required while Microsoft moves each service and associated data for your tenant to a new datacenter geo. Data transfer and validation occur in the background with minimal impact to users. There is no additional cost associated with the migration.

[Learn more about moving data to new Microsoft 365 datacenter regions](#)

☐

I want my organization's core customer data at rest to migrate to Norway by Oct 30, 2022

The text in the **Data residency** will section change to indicate **Your organization has requested to move its data** to the appropriate country and date. You'll also have a confirmation message in your message center. This confirms that you have successfully requested a move.

What happens after requesting a move?

After requesting a move, we will plan to move your core customer data at rest for eligible Microsoft 365 services as quickly as our operational constraints allow. Due to the unpredictable nature of many of the constraints, we cannot share a specific date or timeframe for the moves. Customer tenant administrators will see a notification in Message Center after the move for each service has completed.

Moves may take up to 24 months from the request deadline for your country to complete.

Microsoft Teams

As of January 2020, customers in eligible Office 365 countries can opt-in for migration of Microsoft Teams chat service data. Customers that previously opted-in for a Data Residency move will also have Teams move to their local datacenter geo. No additional action is required by these customers.

Related topics

[Moving core data to new Office 365 datacenter geos](#)

[Data move general FAQ](#)

[New datacenter geos for Microsoft Dynamics CRM Online](#)

[Azure services by region](#)

During and after your data move

10/28/2022 • 5 minutes to read • [Edit Online](#)

Data moves are a back-end operation with minimal impact to end users. No action is required while Microsoft moves each service and associated data for your tenant to a new datacenter geo. Data transfer and validation occur in the background in advance with minimal impact to users.

NOTE

Moves occur at different times for each service. As a result, you'll see the described reduced functionality for each service at a different time.

Watch the Microsoft 365 Message Center for confirmation when moves for each of Exchange Online, SharePoint Online, and Teams chat service complete. As shown in the table below, it can take up to 24 months after the end of the enrollment period to complete core customer data at rest moves to the new datacenter geo.

CUSTOMERS WITH SIGNUP COUNTRY IN	ALL MOVES COMPLETED BY
Australia, New Zealand, Fiji	July 1, 2022
Japan	July 1, 2022
India	July 1, 2022
Canada	July 1, 2022
South Korea	July 1, 2022
United Kingdom	July 1, 2022
France	July 1, 2022
United Arab Emirates	July 1, 2022
South Africa	July 1, 2022
Switzerland, Liechtenstein	July 1, 2022
Norway	November 1, 2022
Germany	May 1, 2023
Brazil	June 1, 2023
Sweden	June 1, 2024
Qatar	March 1, 2025

Exchange Online

Because it takes time to move each user to the new datacenter geo for a single tenant, some users will still be in the old datacenter geo during the move, while others will be in the new datacenter geo. This means that some features that involve accessing multiple mailboxes may not fully work during a period of the move process, which can last weeks. These features are described in the following sections.

Open "Shared Folder" in Outlook Web Access

Some users open a shared mail folder from another mailbox (that the user has read or write permissions to) in Outlook Web Access using the "Shared Folder" feature. The following table describes how access to shared folders works during a mailbox move. Please note that users with full permissions to a shared mailbox can open the mailbox by using Outlook Web Access during the move.

CONFIGURATION	DESCRIPTION
User has mailbox folder permission to another mailbox	Potentially limited. If User A and Mailbox B aren't in the same geo during the tenant move, User A can't open Mailbox B's folder in Outlook Web Access if User A only has permission to a specific folder in Mailbox B. To add a shared folder, right-click the user name in the left navigation panel and select Add shared folder .
User with full mailbox permission to another mailbox	Fully supported. If User A has "Full Access" permission to Mailbox B, then User A can click the shared folder in the left navigation panel in Outlook Web Access to open a window showing Mailbox B. A user can open a shared mailbox using Outlook Web Access during the move without any adverse impact. The limitation only applies to folder-level sharing in a mailbox.

SharePoint Online

When SharePoint Online is moved, data for the following services is also moved:

- OneDrive for Business
- Microsoft 365 Video services
- Office in a browser
- Microsoft 365 Apps for enterprise
- Visio Pro for Microsoft 365

After we've completed moving your SharePoint Online data, you might see some of the following effects.

Microsoft 365 Video Services

- The data move for video takes longer than the moves for the rest of your content in SharePoint Online.
- After the SharePoint Online content is moved, there will be a time frame when videos aren't able to be played.
- We're removing the trans-coded copies from the previous datacenter and transcoding them again in the new datacenter.

Search

In the course of moving your SharePoint Online data, we migrate your search index and search settings to a new location. Until we've **completed** the move of your SharePoint Online data, we continue to serve your users

from the index in the original location. In the new location, search automatically starts crawling your content after we've completed moving your SharePoint Online data. From this point and onwards we serve your users from the migrated index. Changes to your content that occurred after the migration aren't included in the migrated index until crawling picks them up. Most customers don't notice that results are less fresh right after we've completed moving their SharePoint Online data, but some customers might experience reduced freshness in the first 24-48 hours.

The following search features are affected:

- Search results and Search Web Parts: Results don't include changes that occurred after the migration until crawling picks them up.
- Delve: Delve doesn't include changes that occurred after the migration until crawling picks them up.
- Popularity and Search Reports for the site: Counts for Excel reports in the new location only include migrated counts and counts from usage reports that have run after we completed moving your SharePoint Online data. Any counts from the interim period are lost and can't be recovered. This period is typically a couple of days. Some customers might experience shorter or longer losses.
- Video Portal: View counts and statistics for the Video Portal depend on the statistics for Excel Reports, so view counts and statistics for the Video Portal are lost for the same time period as for the Excel reports.
- eDiscovery: Items that changed during the migration aren't shown until crawling picks up the changes.
- Data Loss Protection (DLP): Policies aren't enforced on items that change until crawling picks up the changes.

As part of the migration, the default region will change and all new content will be stored at rest in the new default region. Existing content will move in the background with no impact to you for up to 90 days after the first change to the SharePoint Online data location in the admin center.

Microsoft Teams

Files tab

After the migration is complete the Files tab may take additional time (up to 7 seconds) to fully load when the user first attempts to use it.

Read-only period

Teams chat services moves each thread individually. The thread is locked in a read-only state during the move, which lasts a few seconds per thread. Threads remain accessible during the migration.

Skype for Business

Skype for Business moves are no longer available. [Skype for Business Online will be retired](#) on July 31, 2021. After that time, the service will no longer be accessible.

Related topics

[How to request your data move](#)

[Data move general FAQ](#)

[New datacenter geos for Microsoft Dynamics CRM Online](#)

[Azure services by region](#)

Data move general FAQ

10/28/2022 • 9 minutes to read • [Edit Online](#)

Here are answers to general questions about moving core customer data at rest to a new datacenter geo.

What customers are eligible to request a move?

► [Click to expand](#)

How do we define Core Customer Data?

► [Click to expand](#)

What is in scope for Teams migration?

► [Click to expand](#)

At what point is my migration complete so that my tenant's core customer data is being stored at rest in my new geo?

► [Click to expand](#)

How do you make sure my customer data is safe during the move and that I won't experience downtime?

► [Click to expand](#)

What is the impact of having different services located in different geos?

► [Click to expand](#)

Where is my core customer data located?

► [Click to expand](#)

When will I be able to request a move?

► [Click to expand](#)

How can I request to be moved?

► [Click to expand](#)

Can I change my selection after requesting a move?

► [Click to expand](#)

What happens if I do not request a move before the deadline?

► [Click to expand](#)

What if I want to move my data in order to get better network performance?

► [Click to expand](#)

Do all the services move their data on the same day?

► [Click to expand](#)

Can I choose when I want my data to be moved?

► [Click to expand](#)

Can you share when my data will be moved?

► [Click to expand](#)

What happens if users access services while the data is being moved?

► Click to expand

How do I know the move is complete?

► Click to expand

I am a Microsoft 365 customer in one of the new datacenter geos, but when I signed up, I selected a different country. How can I be moved to the new datacenter geo?

► Click to expand

What happens if we are in process of email data migration to Microsoft 365 during the Exchange Online move?

► Click to expand

Can I pilot some users?

► Click to expand

I don't want to wait for Microsoft to move my data. Can I just create a new tenant and move myself?

► Click to expand

My customer data has already been moved to a new datacenter geo. Can I move back?

► Click to expand

Will Microsoft 365 tenants hosted in the new datacenters be available to users outside of the country?

► Click to expand

My tenant has configured the Multi Geo add-on. Can I still enroll in my tenant in the Microsoft 365 Move Program? to change my default geo and move any user not in a satellite region to the new default geo?

► Click to expand

I have public folders deployed in my tenant. What will be the impact on public folder access during or after the move?

► Click to expand

Related topics

[Moving core data to new Microsoft 365 datacenter geos](#)

[How to request your data move](#)

[Microsoft 365 Multi Geo](#)

[Microsoft 365 interactive datacenter map](#)

[Microsoft 365 Support](#)

[New datacenter geos for Microsoft Dynamics CRM Online](#)

[Azure services by region](#)

Where your Microsoft 365 customer data is stored

10/28/2022 • 176 minutes to read • [Edit Online](#)

The tables below show where customer data is stored at-rest for Microsoft 365 services across all of Microsoft's global cloud locations. Expand the location of your billing address country to find out where customer data for each service would be stored.

If your business is located in the European Union, see [Data locations for the European Union](#) for more information.

Customers should view tenant specific data location information in your Microsoft 365 admin center in **Settings > Org settings > Organization profile tab > Data location**. If you [requested to move to a new Geo](#), the data location information in the Microsoft 365 admin center may show only your new Geo even though some data may be stored temporarily in your prior Geo during the transition.

New Microsoft 365 tenants are defaulted to Geo based on the country of the transaction associated with that tenant's first subscription.

Find information about the contractual commitments for the storage location of customer data at rest in the [Microsoft Products and Services Data Protection Addendum \(DPA\)](#).

For Azure Active Directory data locations, see [Data residency in Azure](#).

If your billing address is outside Europe and you have an Office 365 Education subscription, then notwithstanding the "Location of Customer Data at Rest for Core Online Services" section of the OST, Microsoft may provision your Office 365 tenant in, transfer your data to, and store your data at rest anywhere within Europe or North America. If your billing address is in Europe and you have an Office 365 Education subscription, then notwithstanding the "Location of Customer Data at Rest for Core Online Services" section of the OST, Microsoft may provision your Office 365 tenant in, transfer your data to, and store your data at rest anywhere within the European Union.

FAQ

How does Microsoft define data?

► Click to expand

Where are the exact addresses of the data centers?

► Click to expand

Does the location of your customer data have a direct impact on your end users' experience?

► Click to expand

How does Microsoft help me comply with my national, regional, and industry-specific regulations?

► Click to expand

Who can access your data and according to what rules?

► Click to expand

Does Microsoft access your data?

► Click to expand

How does Microsoft secure your data?

► Click to expand

Does Microsoft 365 encrypt your data?

► Click to expand

Where can I find data residency information for Microsoft Azure?

► Click to expand

What are Multi-Geo Capabilities in Microsoft 365?

► Click to expand

What services support Multi-Geo?

► Click to expand

Why do I see my Microsoft 365 service requests for my data at rest connecting to servers in countries outside of my region?

► Click to expand

What are the exceptions for Intune data locations?

► Click to expand

What are the considerations for Microsoft Viva data locations?

► Click to expand

Data Center Locations

The table below defines the data location for various services. When determining the service locations please refer to these tables.

Data Center Geographies

The following regional geographies can store data at rest. The locations where customer data may be stored can change.

REGIONAL GEOGRAPHIES	LOCATIONS WHERE CUSTOMER DATA MAY BE STORED
Regional Geography 1 – EMEA (Europe, Middle East and Africa)	Austria, Finland, France, Ireland, Netherlands, Sweden
Regional Geography 2 – Asia Pacific	Hong Kong, Japan, Malaysia, Singapore, South Korea
Regional Geography 3 - Americas	Brazil, Chile, United States

Country/Region specific Data Center city locations

For country/region specific data centers, the following defines the cities where customer data is stored at rest.

COUNTRY	CITY
Australia	Sydney, Melbourne
Brazil	Rio, Campinas
Canada	Quebec City, Toronto

COUNTRY	CITY
European Union	Austria (Vienna), Finland (Helsinki), France (Paris, Marseille), Ireland (Dublin), Netherlands (Amsterdam), Sweden (Gävle, Sandviken, Staffanstorpe)
France	Paris, Marseille
Germany	Frankfurt, Berlin
India	Chennai, Mumbai, Pune
Japan	Osaka, Tokyo
Qatar	Doha
South Korea	Busan, Seoul
Norway	Oslo, Stavanger
South Africa	Cape Town, Johannesburg
Sweden	Gävle, Sandviken, Staffanstorpe
Switzerland	Geneva, Zurich
United Arab Emirates	Dubai, Abu Dhabi
United Kingdom	Durham, London, Cardiff
United States	Boydton, Cheyenne, Chicago, Des Moines, Quincy, San Antonio, Santa Clara, San Jose

New Microsoft 365 tenants are defaulted to Geo based on the country of the billing address associated with that tenant's first subscription. To confirm where customer data is stored for existing Office 365 services, please view tenant specific data location information in your Office 365 Admin Center in Settings | Org settings | Organization profile | Data location card. Alternatively, expand the country that your business is based in, from the list below, to find out where customer data would be stored if you were to start using a Microsoft 365 Service today.

Afghanistan

► Click to expand

Aland Islands

► Click to expand

Albania

► Click to expand

Algeria

► [Click to expand](#)

American Samoa

► [Click to expand](#)

Andorra

► [Click to expand](#)

Angola

► [Click to expand](#)

Anguilla

► [Click to expand](#)

Antarctica

► [Click to expand](#)

Antigua and Barbuda

► [Click to expand](#)

Argentina

► [Click to expand](#)

Armenia

► [Click to expand](#)

Aruba

► [Click to expand](#)

Australia

► [Click to expand](#)

Austria

► [Click to expand](#)

Azerbaijan

► [Click to expand](#)

Bahamas

► [Click to expand](#)

Bahrain

► [Click to expand](#)

Bangladesh

► [Click to expand](#)

Barbados

► [Click to expand](#)

Belarus

► [Click to expand](#)

Belgium

► [Click to expand](#)

Belize

► [Click to expand](#)

Benin

► [Click to expand](#)

Bermuda

► [Click to expand](#)

Bhutan

► [Click to expand](#)

Bolivia

► [Click to expand](#)

Bonaire

► [Click to expand](#)

Bosnia and Herzegovina

► [Click to expand](#)

Botswana

► [Click to expand](#)

Bouvet Island

► [Click to expand](#)

Brazil

► [Click to expand](#)

British Indian Ocean Territory

► [Click to expand](#)

British Virgin Islands

► [Click to expand](#)

Brunei

► [Click to expand](#)

Bulgaria

► [Click to expand](#)

Burkina Faso

► [Click to expand](#)

Burundi

► [Click to expand](#)

Cambodia

► [Click to expand](#)

Cameroon

► [Click to expand](#)

Canada

► [Click to expand](#)

Cape Verde

► [Click to expand](#)

Cayman Islands

► [Click to expand](#)

Central African Republic

► [Click to expand](#)

Chad

► [Click to expand](#)

Chile

► [Click to expand](#)

China

► [Click to expand](#)

Christmas Island

► [Click to expand](#)

Cocos (Keeling) Islands

► [Click to expand](#)

Colombia

► [Click to expand](#)

Comoros

► [Click to expand](#)

Congo (Brazzaville)

► [Click to expand](#)

Congo, (Kinshasa)

► [Click to expand](#)

Cook Islands

► [Click to expand](#)

Costa Rica

► [Click to expand](#)

Cote D'Ivoire

► [Click to expand](#)

Croatia

► [Click to expand](#)

Curacao

► [Click to expand](#)

Cyprus

► [Click to expand](#)

Czech Republic

► [Click to expand](#)

Denmark

► [Click to expand](#)

Djibouti

► [Click to expand](#)

Dominica

► [Click to expand](#)

Dominican Republic

► [Click to expand](#)

Ecuador

► [Click to expand](#)

Egypt

► [Click to expand](#)

El Salvador

► [Click to expand](#)

Equatorial Guinea

► [Click to expand](#)

Eritrea

► [Click to expand](#)

Estonia

► [Click to expand](#)

Ethiopia

► [Click to expand](#)

Falkland Islands (Malvinas)

► [Click to expand](#)

Faroe Islands

► [Click to expand](#)

Federated States of Micronesia

► [Click to expand](#)

Fiji

► [Click to expand](#)

Finland

► [Click to expand](#)

France

► [Click to expand](#)

French Guiana

► [Click to expand](#)

French Polynesia

► [Click to expand](#)

French Southern Territories

► [Click to expand](#)

Gabon

► [Click to expand](#)

Gambia

► [Click to expand](#)

Georgia

► [Click to expand](#)

Germany

► [Click to expand](#)

Ghana

► [Click to expand](#)

Gibraltar

► [Click to expand](#)

Greece

► [Click to expand](#)

Greenland

► [Click to expand](#)

Grenada

► [Click to expand](#)

Guadeloupe

► [Click to expand](#)

Guam

► [Click to expand](#)

Guatemala

► [Click to expand](#)

Guernsey

► [Click to expand](#)

Guinea

► [Click to expand](#)

Guinea-Bissau

► [Click to expand](#)

Guyana

► [Click to expand](#)

Haiti

► [Click to expand](#)

Heard and McDonald Islands

► [Click to expand](#)

Herzegovina

► [Click to expand](#)

Holy See (Vatican City State)

► [Click to expand](#)

Honduras

► [Click to expand](#)

Hong Kong SAR

► [Click to expand](#)

Hungary

► [Click to expand](#)

Iceland

► [Click to expand](#)

India

► [Click to expand](#)

Indonesia

► [Click to expand](#)

Iraq

► [Click to expand](#)

Ireland

► [Click to expand](#)

Isle of Man

► [Click to expand](#)

Israel

► [Click to expand](#)

Italy

► [Click to expand](#)

Jamaica

► [Click to expand](#)

Japan

► [Click to expand](#)

Jersey

► [Click to expand](#)

Jordan

► [Click to expand](#)

Kazakhstan

► [Click to expand](#)

Kenya

► [Click to expand](#)

Kiribati

► [Click to expand](#)

South Korea

► [Click to expand](#)

Kosovo

► [Click to expand](#)

Kuwait

► [Click to expand](#)

Kyrgyzstan

► [Click to expand](#)

Laos

► [Click to expand](#)

Latvia

► [Click to expand](#)

Lebanon

► [Click to expand](#)

Lesotho

► [Click to expand](#)

Liberia

► [Click to expand](#)

Libya

► [Click to expand](#)

Liechtenstein

► [Click to expand](#)

Lithuania

► [Click to expand](#)

Luxembourg

► [Click to expand](#)

Madagascar

► [Click to expand](#)

Malawi

► [Click to expand](#)

Malaysia

► [Click to expand](#)

Maldives

► [Click to expand](#)

Mali

► [Click to expand](#)

Malta

► [Click to expand](#)

Marshall Islands

► [Click to expand](#)

Martinique

► [Click to expand](#)

Mauritania

► [Click to expand](#)

Mauritius

► [Click to expand](#)

Mayotte

► [Click to expand](#)

Mexico

► [Click to expand](#)

Moldova

► [Click to expand](#)

Monaco

► [Click to expand](#)

Mongolia

► [Click to expand](#)

Montenegro

► [Click to expand](#)

Montserrat

► [Click to expand](#)

Morocco

► [Click to expand](#)

Mozambique

► [Click to expand](#)

Myanmar

► [Click to expand](#)

Namibia

► [Click to expand](#)

Nauru

► [Click to expand](#)

Nepal

► [Click to expand](#)

Netherlands

► [Click to expand](#)

Netherlands Antilles

► [Click to expand](#)

New Caledonia

► [Click to expand](#)

New Zealand

► [Click to expand](#)

Nicaragua

► [Click to expand](#)

Niger

► [Click to expand](#)

Nigeria

► [Click to expand](#)

Niue

► [Click to expand](#)

Norfolk Island

► [Click to expand](#)

Northern Mariana Islands

► [Click to expand](#)

Norway

► [Click to expand](#)

Oman

► [Click to expand](#)

Pakistan

► [Click to expand](#)

Palau

► [Click to expand](#)

Palestinian Authority

► [Click to expand](#)

Panama

► [Click to expand](#)

Papua New Guinea

► [Click to expand](#)

Paraguay

► [Click to expand](#)

Peru

► [Click to expand](#)

Philippines

► [Click to expand](#)

Pitcairn

► [Click to expand](#)

Poland

► [Click to expand](#)

Portugal

► [Click to expand](#)

Puerto Rico

► [Click to expand](#)

Qatar

► [Click to expand](#)

Republic of Macedonia

► [Click to expand](#)

Réunion

► [Click to expand](#)

Romania

► [Click to expand](#)

Russian Federation

► [Click to expand](#)

Rwanda

► [Click to expand](#)

Saint Helena

► [Click to expand](#)

Saint Kitts and Nevis

► [Click to expand](#)

Saint Lucia

► [Click to expand](#)

Saint Martin

► [Click to expand](#)

Saint Pierre and Miquelon

► [Click to expand](#)

Saint Vincent and the Grenadines

► [Click to expand](#)

Saint-Barthélemy

► [Click to expand](#)

Samoa

► [Click to expand](#)

San Marino

► [Click to expand](#)

Sao Tome and Principe

► [Click to expand](#)

Saudi Arabia

► [Click to expand](#)

Senegal

► [Click to expand](#)

Serbia

► [Click to expand](#)

Seychelles

► [Click to expand](#)

Sierra Leone

► [Click to expand](#)

Singapore

► [Click to expand](#)

Sint Maarten

► [Click to expand](#)

Slovakia

► [Click to expand](#)

Slovenia

► [Click to expand](#)

Solomon Islands

► [Click to expand](#)

Somalia

► [Click to expand](#)

South Africa

► [Click to expand](#)

South Georgia and the South Sandwich Islands

► [Click to expand](#)

Spain

► [Click to expand](#)

Sri Lanka

► [Click to expand](#)

Suriname

► [Click to expand](#)

Svalbard and Jan Mayen Islands

► [Click to expand](#)

Swaziland

► [Click to expand](#)

Sweden

► [Click to expand](#)

Switzerland

► [Click to expand](#)

Taiwan

► [Click to expand](#)

Tajikistan

► [Click to expand](#)

United Republic of Tanzania

► [Click to expand](#)

Thailand

► [Click to expand](#)

Timor-Leste

► [Click to expand](#)

Togo

► [Click to expand](#)

Tokelau

► [Click to expand](#)

Tonga

► [Click to expand](#)

Trinidad and Tobago

► [Click to expand](#)

Tunisia

► [Click to expand](#)

Turkey

► [Click to expand](#)

Turkmenistan

► [Click to expand](#)

Turks and Caicos Islands

► [Click to expand](#)

Tuvalu

► [Click to expand](#)

U.S. Virgin Islands

► [Click to expand](#)

Uganda

► [Click to expand](#)

Ukraine

► [Click to expand](#)

United Arab Emirates

► [Click to expand](#)

United Kingdom

► [Click to expand](#)

United States

► [Click to expand](#)

Uruguay

► [Click to expand](#)

US Minor Outlying Islands

► [Click to expand](#)

Uzbekistan

► [Click to expand](#)

Vanuatu

► [Click to expand](#)

Venezuela

► [Click to expand](#)

Vietnam

► [Click to expand](#)

Wallis and Futuna Islands

► [Click to expand](#)

Western Sahara

► Click to expand

Yemen

► Click to expand

Zambia

► Click to expand

Zimbabwe

► Click to expand

Data locations for the European Union

10/28/2022 • 8 minutes to read • [Edit Online](#)

Your data is your business

Microsoft recognizes the importance of maintaining the privacy and confidentiality of your business data. Your data belongs to you, and you can access, modify, or delete it at any time. Microsoft will not use your data without your consent and, when we have your consent, we use your data to provide only the services you have chosen. If you leave one of our services, we ensure your continued ownership of your data, following strict standards and processes to remove the data from our systems.

NOTE

Customer data (also referred to as "your data" or "your business data") means all data, including text, sound, video or image files, and software that you provide to Microsoft or that's provided on your behalf through your use of Microsoft enterprise online services, excluding Microsoft Professional Services. It includes customer content, which is the data you upload for storage or processing and apps you upload for distribution through a Microsoft enterprise cloud service. For example, customer content includes Exchange Online email and attachments, SharePoint Online site content, or instant messaging conversations.

Data storage and processing

When you use Microsoft 365 services, we start with the assumption that our enterprise customers would like to have their business data stored and processed close to home. Wherever possible, we do just that. To keep your data in datacenters nearest to you, we store your data based on the business location you provide when you create your tenant. To choose storage locations that are meaningful to your organization's businesses, you may create as many tenants for your organization as you would like.

Where EU data is stored

We have datacenter geos in Germany and France that allow you to store data in your country if your business is located there. Our regional European Union data centers are located in Austria, Finland, France, Ireland, and the Netherlands. Your data for the following services will be hosted in the following locations based on which billing address you choose:

SERVICE NAME	LOCATION FOR TENANTS CREATED WITH A BILLING ADDRESS IN FRANCE	LOCATION FOR TENANTS CREATED WITH A BILLING ADDRESS IN GERMANY	LOCATION FOR TENANTS CREATED WITH A BILLING ADDRESS IN ALL OTHER EU COUNTRIES
Exchange Online	France	Germany	European Union
OneDrive for Business	France	Germany	European Union
SharePoint Online	France	Germany	European Union
Skype for Business	European Union	European Union	European Union
Microsoft Teams	France	Germany	European Union
Office Online & Mobile	France	Germany	European Union

SERVICE NAME	LOCATION FOR TENANTS CREATED WITH A BILLING ADDRESS IN FRANCE	LOCATION FOR TENANTS CREATED WITH A BILLING ADDRESS IN GERMANY	LOCATION FOR TENANTS CREATED WITH A BILLING ADDRESS IN ALL OTHER EU COUNTRIES
Exchange Online Protection	France	Germany	European Union
Intune	European Union	European Union	European Union
MyAnalytics	France	Germany	European Union
Planner	European Union	European Union	European Union
Yammer	European Union	European Union	European Union
OneNote Services	France	Germany	European Union
Stream	European Union	European Union	European Union
Whiteboard	European Union	European Union	European Union
Forms	European Union	European Union	European Union

NOTE

If you have an Office 365 Education subscription with a billing address in France or Germany, your data may be stored in our regional European Union datacenters. For the locations of tenant data outside of the EU, see [Where your Microsoft 365 customer data is stored](#).

Where EU data is computed

When you initiate the use of any of the above services, the computations needed to provide the service for your data stored in one of our regional European datacenters (or in your country) will take place within that same geographic boundary unless a temporary data transfer is needed to perform the computation in a Microsoft datacenter located further away.

If a temporary transfer is required, we will always employ state of the art encryption in the transfer and we will always return your data to your chosen data storage location immediately thereafter. We rely on our compliance with European law through the Standard Contractual Clauses (SCCs) for these temporary transfers, along with our supplemental measures to ensure the data is protected.

To learn more, see [European Union Model Clauses](#).

NOTE

Customer data for Sway and Workplace Analytics will be stored and computed in the United States if you elect to use these services.

Microsoft 365 services may query and store portions of tenant directory/identity data information in regions other than the EU where necessary to facilitate certain scenarios. For example, in scenarios of cross regional e-mail routing, call routing and authentication, Microsoft 365 systems may need some information about EU recipients to route these requests properly. Microsoft 365 systems also depend on Azure Active Directory for identity and authentication functions. To learn more, see [Identity data storage for European customers in Azure Active Directory](#).

How Microsoft protects your data

Security measures

Microsoft secures your data using multiple layers of security and encryption protocols. Get an overview of Microsoft data security capabilities in the [Microsoft 365 encryption article](#).

By default, Microsoft Managed Keys protect your customer data. Data that persists on any physical media is always encrypted using FIPS 140-2 compliant encryption protocols. You can also employ customer-managed keys (CMK), [double encryption](#), and/or hardware security modules (HSMs) for increased data protection.

In addition, Microsoft by default uses the [Transport Layer Security \(TLS\)](#) protocol to encrypt data when it's traveling between the cloud services and customers. Microsoft Services negotiate a TLS connection with client systems that connect to Microsoft 365 services.

To prevent unauthorized physical access to datacenters, we employ rigorous operational controls and processes that include 24x7 video monitoring, trained security personnel and processes, and smart card or biometric multifactor access controls. Upon end of life, data disks are shredded and destroyed. If a disk drive used for storage suffers a hardware failure or reaches its end of life, it is securely erased or destroyed. The data on the drive is completely overwritten to ensure the data cannot be recovered by any means. When such devices are decommissioned, they are shredded and destroyed in line with NIST SP 800-88 R1, Guidelines for Media Sanitization. Records of the destruction are retained and reviewed as part of the Microsoft audit and compliance process. All Microsoft 365 services utilize approved media storage and disposal management services.

Technical controls

In addition to the physical and technological protections, Microsoft takes strong measures to help protect your customer data from unauthorized access by Microsoft personnel and subcontractors. Access to customer data by Microsoft operations and support personnel is denied by default. Nearly all service operations performed by Microsoft are fully automated and human involvement is highly controlled and abstracted away from customer data.

Only in rare cases does a Microsoft engineer need access to customer data. Typically this is only necessary if you request Microsoft's assistance to resolve a customer issue. Access to customer data is highly restricted by role-based access controls, multifactor authentication, data minimization and other controls. All access to customer data is strictly logged, and both Microsoft and third parties perform regular audits (as well as sample audits) to attest that any access is appropriate.

Customers can use customer-managed keys to further prevent their data from being readable in case of unauthorized access. Both server-side and client-side encryption can rely on customer-managed keys or customer-provided keys. In either case, Microsoft would not have access to encryption keys and cannot decrypt the data. A SOC audit by an AICPA-accredited auditor twice a year to verifies the effectiveness of our security controls in audit scope. The SOC 2 Type 2 attestation report published by the auditor explains under what circumstances access to customer data can occur and how.

In addition to storing and processing your data when you use the online services, Microsoft generates service data to monitor system health and to perform service operations such as troubleshooting. As a privacy protective measure, Microsoft generates and relies upon pseudonymous identifiers in this service generated data to be able to distinguish one user from another without identifying the actual users. Pseudonymous identifiers don't directly identify a person, and the information that enables mapping pseudonymous identifiers to actual users is protected as part of your data.

To learn more, see [Who can access your data](#) and on what terms and [Subprocessors and Data Privacy](#).

How Microsoft handles government requests

If a government wants customer data, it must follow applicable legal processes. Microsoft must be served with a

warrant or court order for content, or a subpoena for subscriber information or other non-content data.

- All requests must target specific accounts and identifiers.
- Microsoft's legal compliance team reviews all requests to ensure they are valid, rejects those that are not valid, and only provides the data specified.
- If Microsoft is compelled by law to disclose customer data, you will be promptly notified and provided with a copy of the request, unless Microsoft is legally prohibited from doing so.
- Microsoft conducts a local legal review of each request it receives against local laws and standards. Microsoft also periodically reviews its screening processes around the world to ensure local judicial procedures are being followed and its global human rights statement is being applied.

For more information on Microsoft's commitment to challenge orders in line with the EU's GDPR, see [New Steps to Defend Your Data](#).

When governments or law enforcement agencies make a lawful request for customer data, Microsoft is committed to transparency and limits what it discloses. Twice a year, we publish the number of legal demands for customer data that we receive from law enforcement agencies around the world. See [Law Enforcement Requests Report](#). This report does not disclose the specifics of any particular demand, including the customer at issue. Twice a year, we also publish data about the legal demands we receive from the U.S. government. See [US National Security Orders Report](#) for the latest report.

To learn more, see [Frequently Asked Questions](#) regarding government and law enforcement requests, including questions about the CLOUD Act.

Additional resources

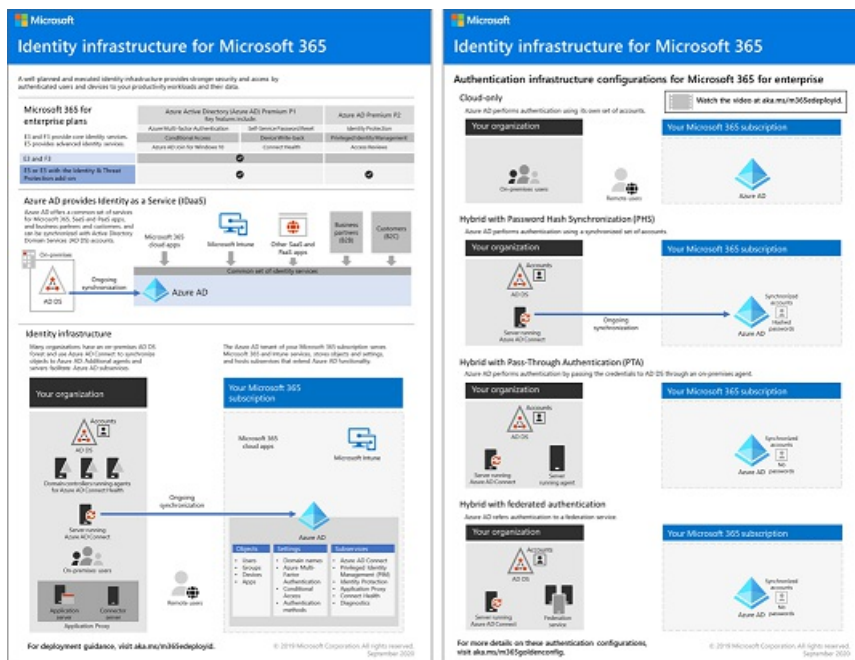
- [Trusted data protection](#) provides an overview of how Microsoft protects your data when you use Microsoft Online Services and Professional Services. It's also suggested that you consult the [Microsoft Online Services Terms \(OST\)](#) and [Data Protection Addendum \(DPA\)](#) that govern your use of these services.
- [Office 365 Data Subject Requests for the GDPR](#) helps you find and act on personal data or personal information to respond to DSRs using Microsoft 365 products, services, and administrative tools.
- [Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365](#) helps you determine whether your organization needs to draft a DPIA, provides "how to" guidance, includes a customizable DPIA template document, and provides a DPIA Service Elements Matrix for many Microsoft 365 services.
- [Learn how modules](#) are designed for people in audit, compliance, risk, and legal roles who seek an overall understanding provide an in-depth review of how Microsoft 365's fundamental security and privacy practices to safeguard customer data.
- [Microsoft Compliance Offerings](#) shows how Microsoft 365 services help your organization meet regulatory compliance standards.

Deploy your identity infrastructure for Microsoft 365

10/28/2022 • 4 minutes to read • [Edit Online](#)

In Microsoft 365 for enterprise, a well-planned and executed identity infrastructure paves the way for stronger security, including restricting access to your productivity workloads and their data to only authenticated users and devices. Security for identities is a key element of a Zero Trust deployment, in which all attempts to access resources both on-premises and in the cloud are authenticated and authorized.

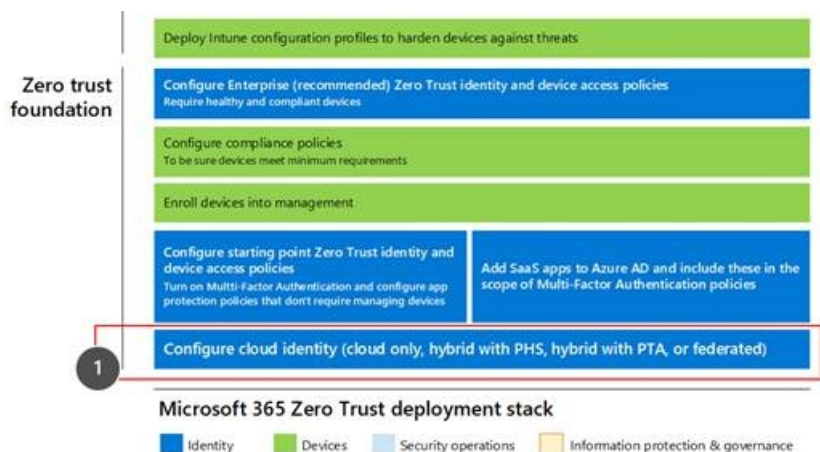
For information about the identity features of each Microsoft 365 for enterprise, the role of Azure Active Directory (Azure AD), on-premises and cloud-based components, and the most common authentication configurations, see the [Identity Infrastructure poster](#).



Review this two-page poster to quickly ramp up on identity concepts and configurations for Microsoft 365 for enterprise.

You can [download this poster](#) and can print it in letter, legal, or tabloid (11 x 17) format.

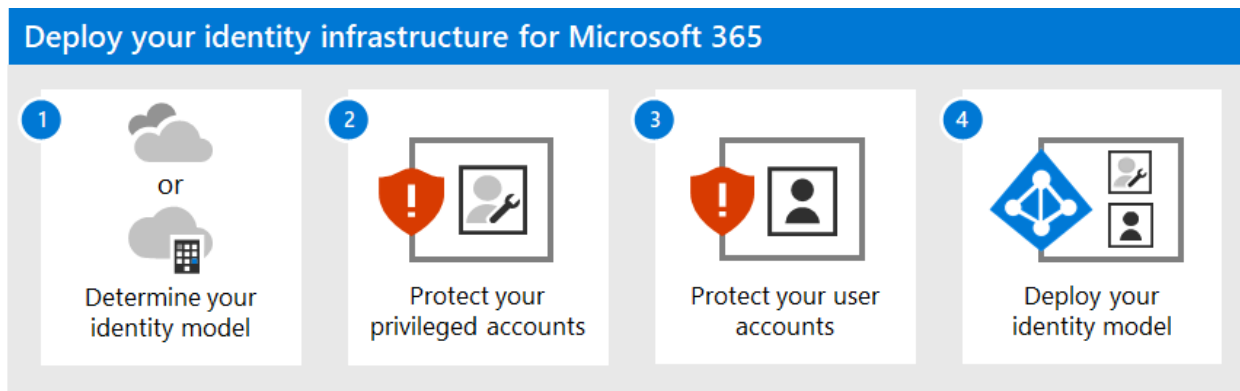
This solution is the first step to build out the Microsoft 365 Zero Trust deployment stack.



For more information, see the [Microsoft 365 Zero Trust deployment plan](#).

What's in this solution

This solution steps you through the deployment of an identity infrastructure for your Microsoft 365 tenant to provide access for your employees and protection against identity-based attacks.



The steps in this solution are:

1. [Determine your identity model.](#)
2. [Protect your Microsoft 365 privileged accounts.](#)
3. [Protect your Microsoft 365 user accounts.](#)
4. [Deploy your identity model.](#)

This solution supports the key principles of [Zero Trust](#):

- **Verify explicitly:** Always authenticate and authorize based on all available data points.
- **Use least privilege access:** Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
- **Assume breach:** Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Unlike conventional intranet access, which trusts everything behind an organization's firewall, Zero Trust treats each sign-in and access as though it originated from an uncontrolled network, whether it's behind the organization firewall or on the Internet. Zero Trust requires protection for the network, infrastructure, identities, endpoints, apps, and data.

Microsoft 365 capabilities and features

Azure AD provides a full suite of identity management and security capabilities for your Microsoft 365 tenant.

CAPABILITY OR FEATURE	DESCRIPTION	LICENSING
Multi-factor authentication (MFA)	MFA requires users to provide two forms of verification, such as a user password plus a notification from the Microsoft Authenticator app or a phone call. MFA greatly reduces the risk that stolen credentials can be used to access your environment. Microsoft 365 uses the Azure AD Multi-Factor Authentication service for MFA-based sign-ins.	Microsoft 365 E3 or E5

CAPABILITY OR FEATURE	DESCRIPTION	LICENSING
Conditional Access	Azure AD evaluates the conditions of the user sign-in and uses Conditional Access policies to determine the allowed access. For example, in this guidance we show you how to create a Conditional Access policy to require device compliance for access to sensitive data. This greatly reduces the risk that a hacker with their own device and stolen credentials can access your sensitive data. It also protects sensitive data on the devices, because the devices must meet specific requirements for health and security.	Microsoft 365 E3 or E5
Azure AD groups	Conditional Access policies, device management with Intune, and even permissions to files and sites in your organization rely on the assignment to user accounts or Azure AD groups. We recommend you create Azure AD groups that correspond to the levels of protection you are implementing. For example, your executive staff are likely higher value targets for hackers. Therefore, it makes sense to add the user accounts of these employees to an Azure AD group and assign this group to Conditional Access policies and other policies that enforce a higher level of protection for access.	Microsoft 365 E3 or E5
Azure AD Identity Protection	Enables you to detect potential vulnerabilities affecting your organization's identities and configure automated remediation policy to low, medium, and high sign-in risk and user risk. This guidance relies on this risk evaluation to apply Conditional Access policies for multi-factor authentication. This guidance also includes a Conditional Access policy that requires users to change their password if high-risk activity is detected for their account.	Microsoft 365 E5, Microsoft 365 E3 with the E5 Security add-on, EMS E5, or Azure AD Premium P2 licenses
Self-service password reset (SSPR)	Allow your users to reset their passwords securely and without help-desk intervention, by providing verification of multiple authentication methods that the administrator can control.	Microsoft 365 E3 or E5

CAPABILITY OR FEATURE	DESCRIPTION	LICENSING
Azure AD password protection	Detect and block known weak passwords and their variants and additional weak terms that are specific to your organization. Default global banned password lists are automatically applied to all users in an Azure AD tenant. You can define additional entries in a custom banned password list. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.	Microsoft 365 E3 or E5

Next steps

Use these steps to deploy an identity model and authentication infrastructure for your Microsoft 365 tenant:

1. [Determine your cloud identity model.](#)
2. [Protect your Microsoft 365 privileged accounts.](#)
3. [Protect your Microsoft 365 user accounts.](#)
4. Deploy your cloud identity model: [cloud-only](#) or [hybrid](#).



Additional Microsoft cloud identity resources

Manage

To manage your Microsoft cloud identity deployment, see:

- [User accounts](#)
- [Licenses](#)
- [Passwords](#)
- [Groups](#)
- [Governance](#)
- [Directory synchronization](#)

How Microsoft does identity for Microsoft 365

Learn how IT experts at Microsoft [manage identities and secure access](#).

NOTE

This IT Showcase resource is available only in English.

How Contoso did identity for Microsoft 365

For an example of how a fictional but representative multinational organization has deployed a hybrid identity infrastructure for Microsoft 365 cloud services, see [Identity for the Contoso Corporation](#).

Step 1. Determine your cloud identity model

10/28/2022 • 6 minutes to read • [Edit Online](#)

Microsoft 365 uses Azure Active Directory (Azure AD), a cloud-based user identity and authentication service that is included with your Microsoft 365 subscription, to manage identities and authentication for Microsoft 365. Getting your identity infrastructure configured correctly is vital to managing Microsoft 365 user access and permissions for your organization.

Before you begin, watch this video for an overview of identity models and authentication for Microsoft 365.

Your first planning choice is your cloud identity model.

Microsoft cloud identity models

To plan for user accounts, you first need to understand the two identity models in Microsoft 365. You can maintain your organization's identities only in the cloud, or you can maintain your on-premises Active Directory Domain Services (AD DS) identities and use them for authentication when users access Microsoft 365 cloud services.

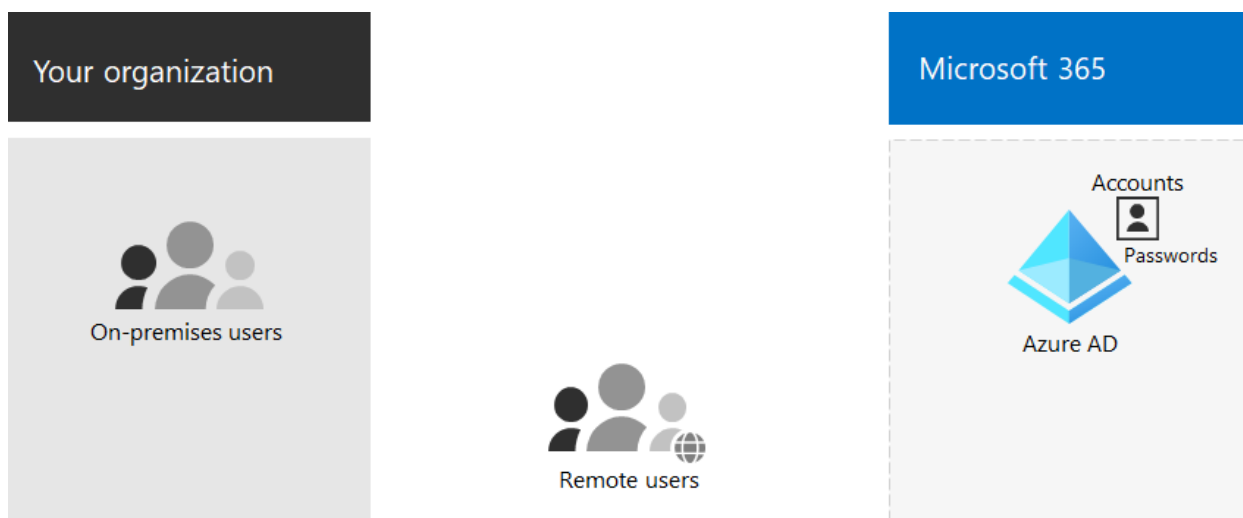
Here are the two types of identity and their best fit and benefits.

ATTRIBUTE	CLOUD-ONLY IDENTITY	HYBRID IDENTITY
Definition	User account only exists in the Azure AD tenant for your Microsoft 365 subscription.	User account exists in AD DS and a copy is also in the Azure AD tenant for your Microsoft 365 subscription. The user account in Azure AD might also include a hashed version of the already hashed AD DS user account password.
How Microsoft 365 authenticates user credentials	The Azure AD tenant for your Microsoft 365 subscription performs the authentication with the cloud identity account.	The Azure AD tenant for your Microsoft 365 subscription either handles the authentication process or redirects the user to another identity provider.
Best for	Organizations that do not have or need an on-premises AD DS.	Organizations using AD DS or another identity provider.
Greatest benefit	Simple to use. No extra directory tools or servers required.	Users can use the same credentials when accessing on-premises or cloud-based resources.

Cloud-only identity

A cloud-only identity uses user accounts that exist only in Azure AD. Cloud-only identity is typically used by small organizations that do not have on-premises servers or do not use AD DS to manage local identities.

Here are the basic components of cloud-only identity.



Both on-premises and remote (online) users use their Azure AD user accounts and passwords to access Microsoft 365 cloud services. Azure AD authenticates user credentials based on its stored user accounts and passwords.

Administration

Because user accounts are only stored in Azure AD, you manage cloud identities with tools such as the [Microsoft 365 admin center](#) and [Windows PowerShell](#).

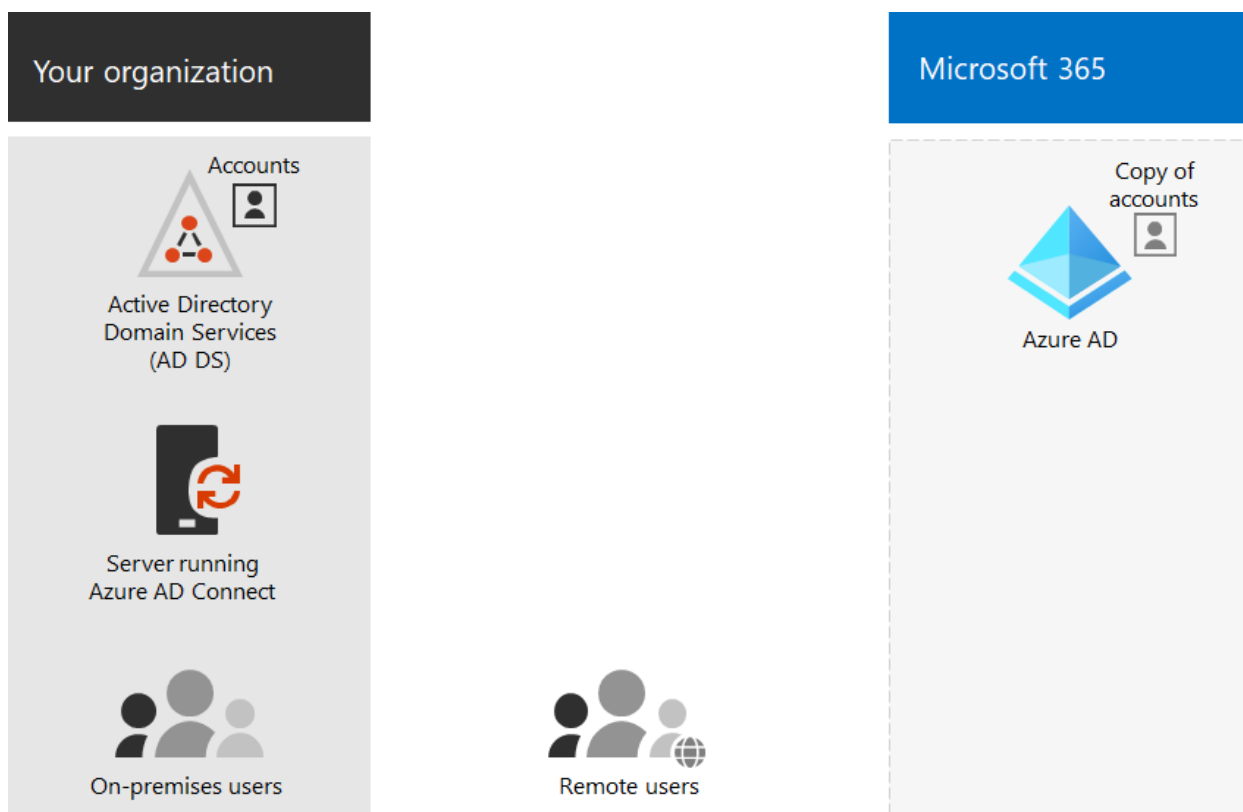
Hybrid identity

Hybrid identity uses accounts that originate in an on-premises AD DS and have a copy in the Azure AD tenant of a Microsoft 365 subscription. Most changes, with the exception of [specific account attributes](#), only flow one way. Changes that you make to AD DS user accounts are synchronized to their copy in Azure AD.

Azure AD Connect provides the ongoing account synchronization. It runs on an on-premises server, checks for changes in the AD DS, and forwards those changes to Azure AD. Azure AD Connect provides the ability to filter which accounts are synchronized and whether to synchronize a hashed version of user passwords, known as password hash synchronization (PHS).

When you implement hybrid identity, your on-premises AD DS is the authoritative source for account information. This means that you perform administration tasks mostly on-premises, which are then synchronized to Azure AD.

Here are the components of hybrid identity.



The Azure AD tenant has a copy of the AD DS accounts. In this configuration, both on-premises and remote users accessing Microsoft 365 cloud services authenticate against Azure AD.

NOTE

You always need to use Azure AD Connect to synchronize user accounts for hybrid identity. You need the synchronized user accounts in Azure AD to perform license assignment and group management, configure permissions, and other administrative tasks that involve user accounts.

Hybrid identity and directory synchronization for Microsoft 365

Depending on your business needs and technical requirements, the hybrid identity model and directory synchronization is the most common choice for enterprise customers who are adopting Microsoft 365. Directory synchronization allows you to manage identities in your Active Directory Domain Services (AD DS) and all updates to user accounts, groups, and contacts are synchronized to the Azure Active Directory (Azure AD) tenant of your Microsoft 365 subscription.

NOTE

When AD DS user accounts are synchronized for the first time, they are not automatically assigned a Microsoft 365 license and cannot access Microsoft 365 services, such as email. You must first assign them a usage location. Then, assign a license to these user accounts, either individually or dynamically through group membership.

Authentication for hybrid identity

There are two types of authentication when using the hybrid identity model:

- Managed authentication

Azure AD handles the authentication process by using a locally-stored hashed version of the password or sends the credentials to an on-premises software agent to be authenticated by the on-premises AD DS.

- Federated authentication

Azure AD redirects the client computer requesting authentication to another identity provider.

Managed authentication

There are two types of managed authentication:

- Password hash synchronization (PHS)

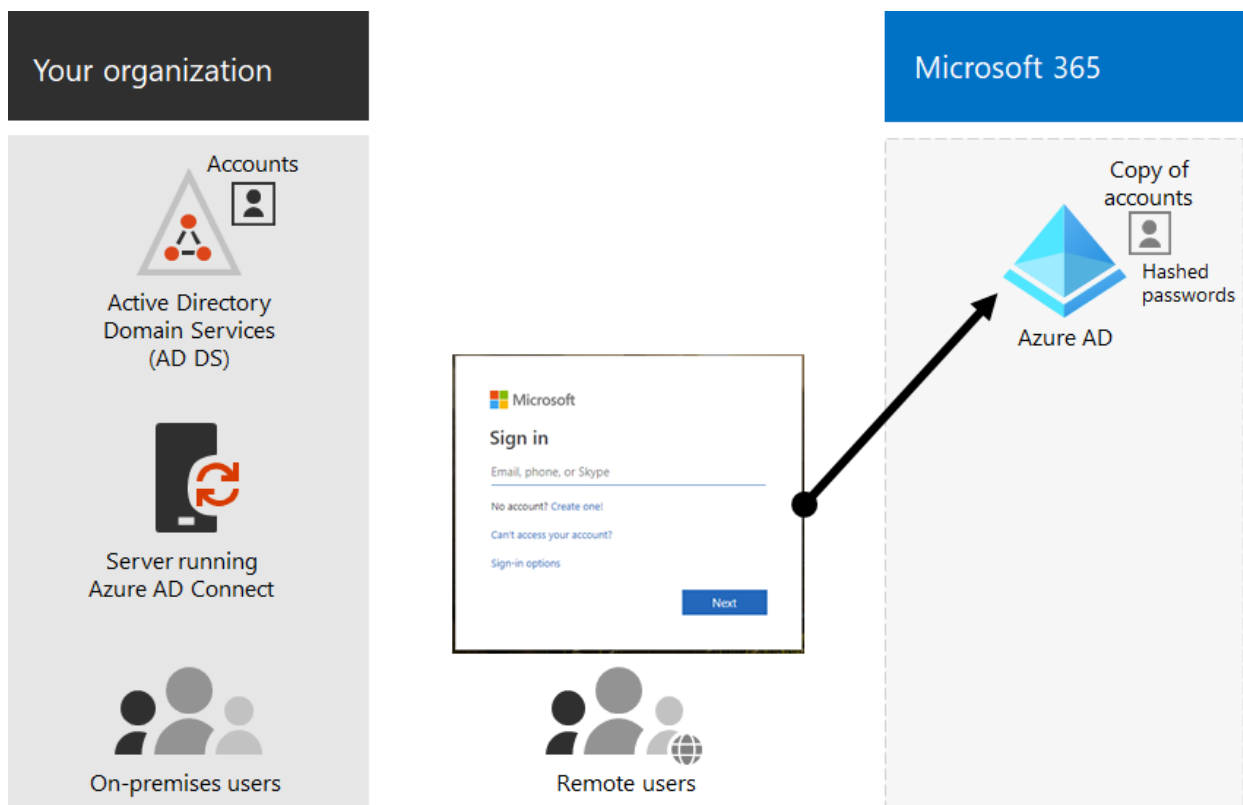
Azure AD performs the authentication itself.

- Pass-through authentication (PTA)

Azure AD has AD DS perform the authentication.

Password hash synchronization (PHS)

With PHS, you synchronize your AD DS user accounts with Microsoft 365 and manage your users on-premises. Hashes of user passwords are synchronized from your AD DS to Azure AD so that the users have the same password on-premises and in the cloud. This is the simplest way to enable authentication for AD DS identities in Azure AD.

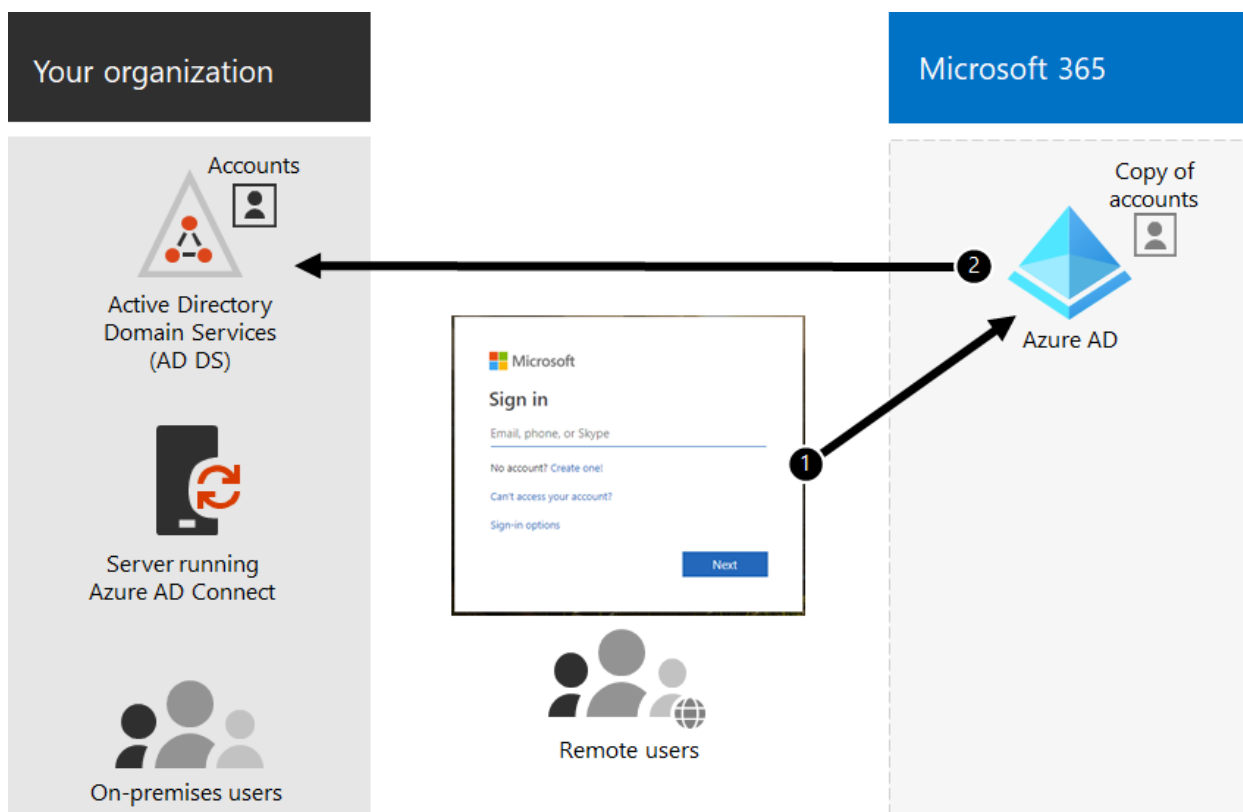


When passwords are changed or reset on-premises, the new password hashes are synchronized to Azure AD so that your users can always use the same password for cloud resources and on-premises resources. The user passwords are never sent to Azure AD or stored in Azure AD in clear text. Some premium features of Azure AD, such as Identity Protection, require PHS regardless of which authentication method is selected.

See [choosing the right authentication method](#) to learn more.

Pass-through authentication (PTA)

PTA provides a simple password validation for Azure AD authentication services using a software agent running on one or more on-premises servers to validate the users directly with your AD DS. With PTA, you synchronize AD DS user accounts with Microsoft 365 and manage your users on-premises.



PTA allows your users to sign in to both on-premises and Microsoft 365 resources and applications using their on-premises account and password. This configuration validates users passwords directly against your on-premises AD DS without storing password hashes in Azure AD.

PTA is also for organizations with a security requirement to immediately enforce on-premises user account states, password policies, and logon hours.

See [choosing the right authentication method](#) to learn more.

Federated authentication

Federated authentication is primarily for large enterprise organizations with more complex authentication requirements. AD DS identities are synchronized with Microsoft 365 and users accounts are managed on-premises. With federated authentication, users have the same password on-premises and in the cloud and they do not have to sign in again to use Microsoft 365.

Federated authentication can support additional authentication requirements, such as smartcard-based authentication or a third-party multi-factor authentication and is typically required when organizations have an authentication requirement not natively supported by Azure AD.

See [choosing the right authentication method](#) to learn more.

For third-party authentication and identity providers, on-premises directory objects may be synchronized to Microsoft 365 and cloud resource access that are primarily managed by a third-party identity provider (IdP). If your organization uses a third-party federation solution, you can configure sign-on with that solution for Microsoft 365 provided that the third-party federation solution is compatible with Azure AD.

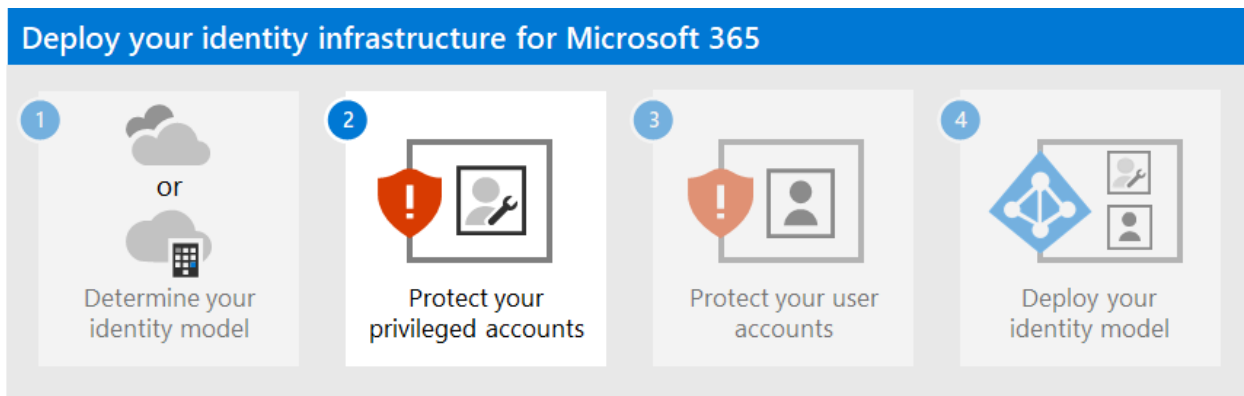
See the [Azure AD federation compatibility list](#) to learn more.

Administration

Because the original and authoritative user accounts are stored in the on-premises AD DS, you manage your identities with the same tools as you manage your AD DS.

You don't use the Microsoft 365 admin center or PowerShell for Microsoft 365 to manage synchronized user accounts in Azure AD.

Next step



Continue with [Step 2](#) to secure your global administrator accounts.

Step 2. Protect your Microsoft 365 privileged accounts

10/28/2022 • 6 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Security breaches of a Microsoft 365 tenant, including information harvesting and phishing attacks, are typically done by compromising the credentials of a Microsoft 365 privileged account. Security in the cloud is a partnership between you and Microsoft:

- Microsoft cloud services are built on a foundation of trust and security. Microsoft provides you security controls and capabilities to help you protect your data and applications.
- You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control.

Microsoft provides capabilities to help protect your organization, but they're effective only if you use them. If you don't use them, you may be vulnerable to attack. To protect your privileged accounts, Microsoft is here to help you with detailed instructions to:

1. Create dedicated, privileged, cloud-based accounts and use them only when necessary.
2. Configure multi-factor authentication (MFA) for your dedicated Microsoft 365 privileged accounts and use the strongest form of secondary authentication.
3. Protect privileged accounts with Zero Trust identity and device access recommendations.

NOTE

To secure your privileged roles, check out [Best practices for Azure AD roles](#) to secure privileged access to your tenant.

1. Create dedicated, privileged, cloud-based user accounts and use them only when necessary

Instead of using everyday user accounts that have been assigned administrator roles, create dedicated user accounts that have the admin roles in Azure AD.

From this moment onward, you sign in with the dedicated privileged accounts only for tasks that require administrator privileges. All other Microsoft 365 administration must be done by assigning other administration roles to user accounts.

NOTE

This does require additional steps to sign out as your everyday user account and sign in with a dedicated administrator account. But this only needs to be done occasionally for administrator operations. Consider that recovering your Microsoft 365 subscription after an administrator account breach requires a lot more steps.

You also need to create [emergency access accounts](#) to prevent being accidentally locked out of Azure AD.

You can further protect your privileged accounts with Azure AD Privileged Identity Management (PIM) for on-demand, just-in-time assignment of administrator roles.

2. Configure multi-factor authentication for your dedicated Microsoft 365 privileged accounts

Multi-factor authentication (MFA) requires additional information beyond the account name and password. Microsoft 365 supports these extra verification methods:

- The Microsoft Authenticator app
- A phone call
- A randomly generated verification code sent through a text message
- A smart card (virtual or physical) (requires federated authentication)
- A biometric device
- Oauth token

NOTE

For organizations that must adhere to National Institute of Standards and Technology (NIST) standards, the use of a phone call or text message-based additional verification methods are restricted. Click [here](#) for the details.

If you're a small business that is using user accounts stored only in the cloud (the cloud-only identity model), [set up MFA](#) to configure MFA using a phone call or a text message verification code sent to a smart phone for each dedicated privileged account.

If you're a larger organization that is using a Microsoft 365 hybrid identity model, you have more verification options. If you have the security infrastructure already in place for a stronger secondary authentication method, [set up MFA](#) and configure each dedicated privileged account for the appropriate verification method.

If the security infrastructure for the desired stronger verification method isn't in place and functioning for Microsoft 365 MFA, we strongly recommend that you configure dedicated privileged accounts with MFA using the Microsoft Authenticator app, a phone call, or a text message verification code sent to a smart phone for your privileged accounts as an interim security measure. Don't leave your dedicated privileged accounts without the extra protection provided by MFA.

For more information, see [MFA for Microsoft 365](#).

3. Protect administrator accounts with Zero Trust identity and device access recommendations

To help ensure a secure and productive workforce, Microsoft provides a set of recommendations for [identity and device access](#). For identity, use the recommendations and settings in these articles:

- [Prerequisites](#)
- [Common identity and device access policies](#)

Additional protections for enterprise organizations

Use these additional methods to ensure that your privileged account, and the configuration that you perform using it, are as secure as possible.

Privileged access workstation

To ensure that the execution of highly privileged tasks is as secure as possible, use a privileged access workstation (PAW). A PAW is a dedicated computer that is only used for sensitive configuration tasks, such as Microsoft 365 configuration that requires a privileged account. Because this computer isn't used daily for Internet browsing or email, it's better protected from Internet attacks and threats.

For instructions on how to set up a PAW, see <https://aka.ms/cyberpaw>.

To enable Azure PIM for your Azure AD tenant and administrator accounts, see the [steps to configure PIM](#).

To develop a comprehensive roadmap to secure privileged access against cyber attackers, see [Securing privileged access for hybrid and cloud deployments in Azure AD](#).

Azure AD Privileged Identity Management

Rather than having your privileged accounts be permanently assigned an administrator role, you can use Azure AD PIM to enable on-demand, just-in-time assignment of the administrator role when it's needed.

Your administrator accounts go from being permanent admins to eligible admins. The administrator role is inactive until someone needs it. You then complete an activation process to add the administrator role to the privileged account for a predetermined amount of time. When the time expires, PIM removes the administrator role from the privileged account.

Using PIM and this process significantly reduces the amount of time that your privileged accounts are vulnerable to attack and use by malicious users.

PIM is available with Azure Active Directory Premium P2, which is included with Microsoft 365 E5. Alternately, you can purchase individual Azure Active Directory Premium P2 licenses for your administrator accounts.

For more information, see:

- [Azure AD Privileged Identity Management](#).
- [Securing privileged access for hybrid and cloud deployments in Azure AD](#)

Privileged access management

Privileged access management is enabled by configuring policies that specify just-in-time access for task-based activities in your tenant. It can help protect your organization from breaches that may use existing privileged administrator accounts with standing access to sensitive data or access to critical configuration settings. For example, you could configure a privileged access management policy that requires explicit approval to access and change organization mailbox settings in your tenant.

In this step, you'll enable privileged access management in your tenant and configure privileged access policies that provide extra security for task-based access to data and configuration settings for your organization. There are three basic steps to get started with privileged access in your organization:

- Creating an approver's group
- Enabling privileged access
- Creating approval policies

Privileged access management enables your organization to operate with zero standing privileges and provide a layer of defense against vulnerabilities arising because of such standing administrative access. Privileged access requires approvals for executing any task that has an associated approval policy defined. Users needing to execute tasks included in the approval policy must request and be granted access approval.

To enable privileged access management, see [Configure privileged access management](#).

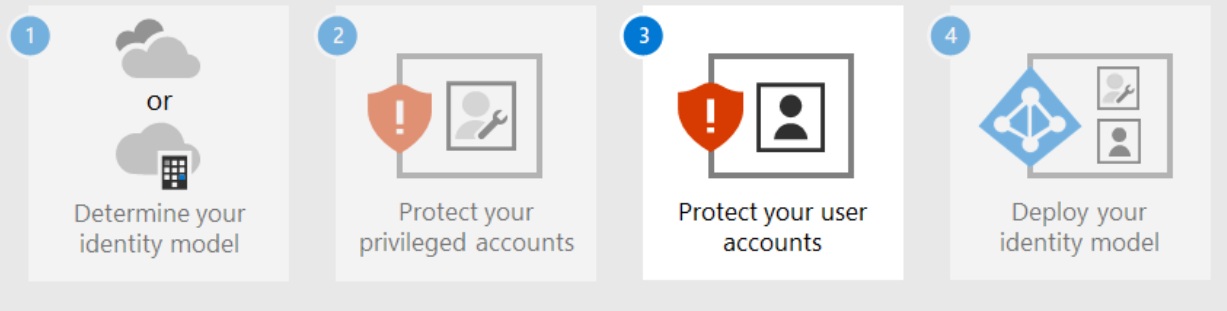
For more information, see [Privileged access management](#).

Security information and event management (SIEM) software for Microsoft 365 logging

SIEM software run on a server performs real-time analysis of security alerts and events created by applications and network hardware. To allow your SIEM server to include Microsoft 365 security alerts and events in its analysis and reporting functions, integrate Azure AD into your SIEM. See [Introduction to Azure Log Integration](#).

Next step

Deploy your identity infrastructure for Microsoft 365



Continue with [Step 3](#) to secure your user accounts.

Step 3: Protect your Microsoft 365 user accounts

10/28/2022 • 6 minutes to read • [Edit Online](#)

To increase the security of user sign-ins:

- Use Windows Hello for Business
- Use Azure Active Directory (Azure AD) Password Protection
- Use multi-factor authentication (MFA)
- Deploy identity and device access configurations
- Protect against credential compromise with Azure AD Identity Protection

Windows Hello for Business

Windows Hello for Business in Windows 10 Enterprise replaces passwords with strong two-factor authentication when signing on a Windows device. The two factors are a new type of user credential that is tied to a device and a biometric or PIN.

For more information, see [Windows Hello for Business Overview](#).

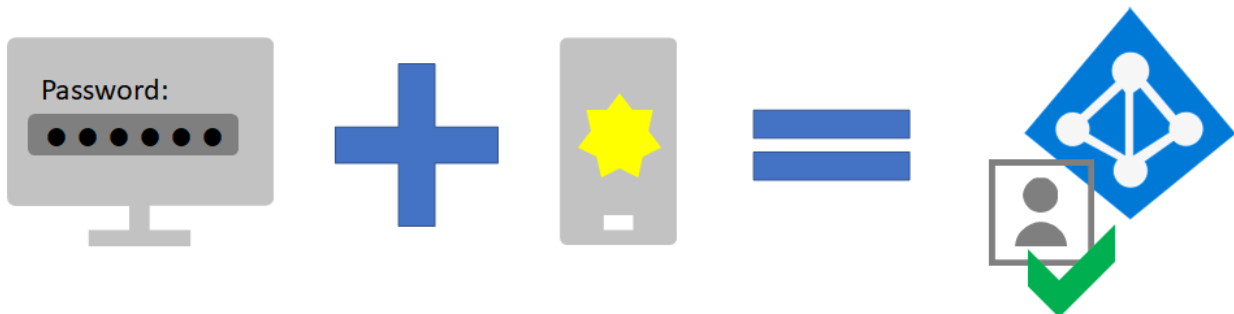
Azure AD Password Protection

Azure AD Password Protection detects and blocks known weak passwords and their variants and can also block additional weak terms that are specific to your organization. Default global banned password lists are automatically applied to all users in an Azure AD tenant. You can define additional entries in a custom banned password list. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

For more information, see [Configure Azure AD password protection](#).

MFA

MFA requires that user sign-ins be subject to an additional verification beyond the user account password. Even if a malicious user determines a user account password, they must also be able to respond to an additional verification, such as a text message sent to a smartphone before access is granted.



Your first step in using MFA is to [require it for all administrator accounts](#), also known as privileged accounts. Beyond this first step, Microsoft recommends MFA For all users.

There are three ways to require your users to use MFA based on your Microsoft 365 plan.

PLAN	RECOMMENDATION
All Microsoft 365 plans (without Azure AD Premium P1 or P2 licenses)	Enable security defaults in Azure AD . Security defaults in Azure AD include MFA for users and administrators.
Microsoft 365 E3 (includes Azure AD Premium P1 licenses)	Use the common Conditional Access policies to configure the following policies: - Require MFA for administrators - Require MFA for all users - Block legacy authentication
Microsoft 365 E5 (includes Azure AD Premium P2 licenses)	Taking advantage of Azure AD Identity Protection, begin to implement Microsoft's recommended set of Conditional Access and related policies by creating these two policies: - Require MFA when sign-in risk is medium or high - High risk users must change password

Security defaults

Security defaults is a new feature for Microsoft 365 and Office 365 paid or trial subscriptions created after October 21, 2019. These subscriptions have security defaults turned on, which ***requires all of your users to use MFA with the Microsoft Authenticator app.***

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Security defaults ensure that all organizations have a basic level of security for user sign-in that is enabled by default. You can disable security defaults in favor of MFA with Conditional Access policies or for individual accounts.

For more information, see the [overview of security defaults](#).

Conditional Access policies

Conditional Access policies are a set of rules that specify the conditions under which sign-ins are evaluated and access is granted. For example, you can create a Conditional Access policy that states:

- If the user account name is a member of a group for users that are assigned the Exchange, user, password, security, SharePoint, **Exchange admin**, **SharePoint admin**, or **Global admin** roles, require MFA before allowing access.

This policy allows you to require MFA based on group membership, rather than trying to configure individual user accounts for MFA when they are assigned or unassigned from these administrator roles.

You can also use Conditional Access policies for more advanced capabilities, such as requiring that the sign-in is done from a compliant device, such as your laptop running Windows 10.

Conditional Access requires Azure AD Premium P1 licenses, which are included with Microsoft 365 E3 and E5.

For more information, see the [overview of Conditional Access](#).

Using these methods together

Keep the following in mind:

- You cannot enable security defaults if you have any Conditional Access policies enabled.
- You cannot enable any Conditional Access policies if you have security defaults enabled.

If security defaults are enabled, all new users are prompted for MFA registration and the use of the Microsoft

Authenticator app.

This table shows the results of enabling MFA with security defaults and Conditional Access policies.

METHOD	ENABLED	DISABLED	ADDITIONAL AUTHENTICATION METHOD
Security defaults	Can't use Conditional Access policies	Can use Conditional Access policies	Microsoft Authenticator app
Conditional Access policies	If any are enabled, you can't enable security defaults	If all are disabled, you can enable security defaults	User specifies during MFA registration

Zero Trust identity and device access configurations

Zero Trust identity and device access settings and policies are recommended prerequisite features and their settings combined with Conditional Access, Intune, and Azure AD Identity Protection policies that determine whether a given access request should be granted and under what conditions. This determination is based on the user account of the sign-in, the device being used, the app the user is using for access, the location from which the access request is made, and an assessment of the risk of the request. This capability helps ensure that only approved users and devices can access your critical resources.

NOTE

Azure AD Identity Protection requires Azure AD Premium P2 licenses, which are included with Microsoft 365 E5.

Identity and device access policies are defined to be used in three tiers:

- Baseline protection is a minimum level of security for your identities and devices that access your apps and data.
- Sensitive protection provides additional security for specific data. Identities and devices are subject to higher levels of security and device health requirements.
- Protection for environments with highly regulated or classified data is for typically small amounts of data that are highly classified, contain trade secrets, or is subject to data regulations. Identities and devices are subject to much higher levels of security and device health requirements.

These tiers and their corresponding configurations provide consistent levels of protection across your data, identities, and devices.

Microsoft highly recommends configuring and rolling out Zero Trust identity and device access policies in your organization, including specific settings for Microsoft Teams, Exchange Online, and SharePoint. For more information, see [Zero Trust identity and device access configurations](#).

Azure AD Identity Protection

In this section, you'll learn how to configure policies that protect against credential compromise, where an attacker determines a user's account name and password to gain access to an organization's cloud services and data. Azure AD Identity Protection provides a number of ways to help prevent an attacker from compromising a user account's credentials.

With Azure AD Identity Protection, you can:

CAPABILITY	DESCRIPTION
Determine and address potential vulnerabilities in your organization's identities	Azure AD uses machine learning to detect anomalies and suspicious activity, such as sign-ins and post-sign-in activities. Using this data, Azure AD Identity Protection generates reports and alerts that help you evaluate the issues and take action.
Detect suspicious actions that are related to your organization's identities and respond to them automatically	You can configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached. These policies, in addition to other Conditional Access controls provided by Azure AD and Microsoft Intune, can either automatically block access or take corrective actions, including password resets and requiring Azure AD Multi-Factor Authentication for subsequent sign-ins.
Investigate suspicious incidents and resolve them with administrative actions	You can investigate risk events using information about the security incident. Basic workflows are available to track investigations and initiate remediation actions, such as password resets.

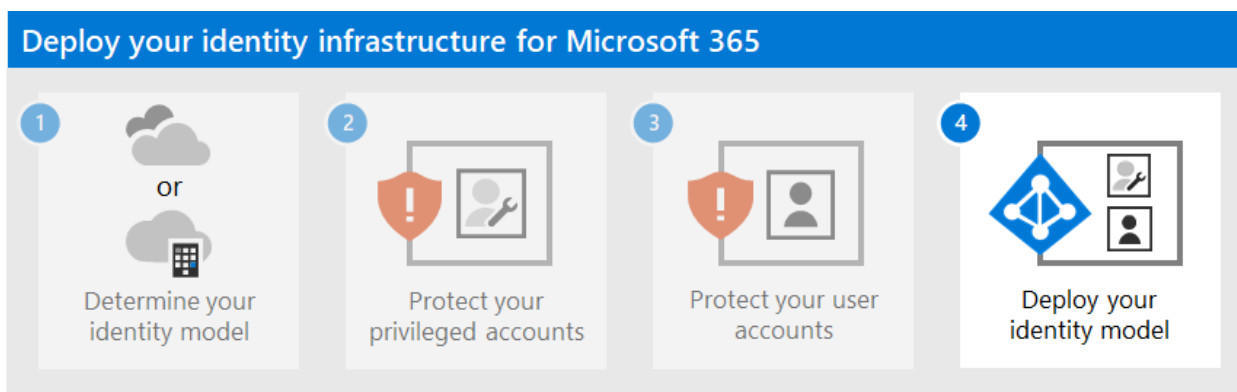
See [more information about Azure AD Identity Protection](#).

See the [steps to enable Azure AD Identity Protection](#).

Admin technical resources for MFA and secure sign-ins

- [MFA for Microsoft 365](#)
- [Deploy identity for Microsoft 365](#)
- [Azure Academy Azure AD training videos](#)
- [Configure the Azure AD Multi-Factor Authentication registration policy](#)
- [Identity and device access configurations](#)

Next step



Continue with Step 4 to deploy the identity infrastructure based on your chosen identity model:

- [Cloud-only identity](#)
- [Hybrid identity](#)

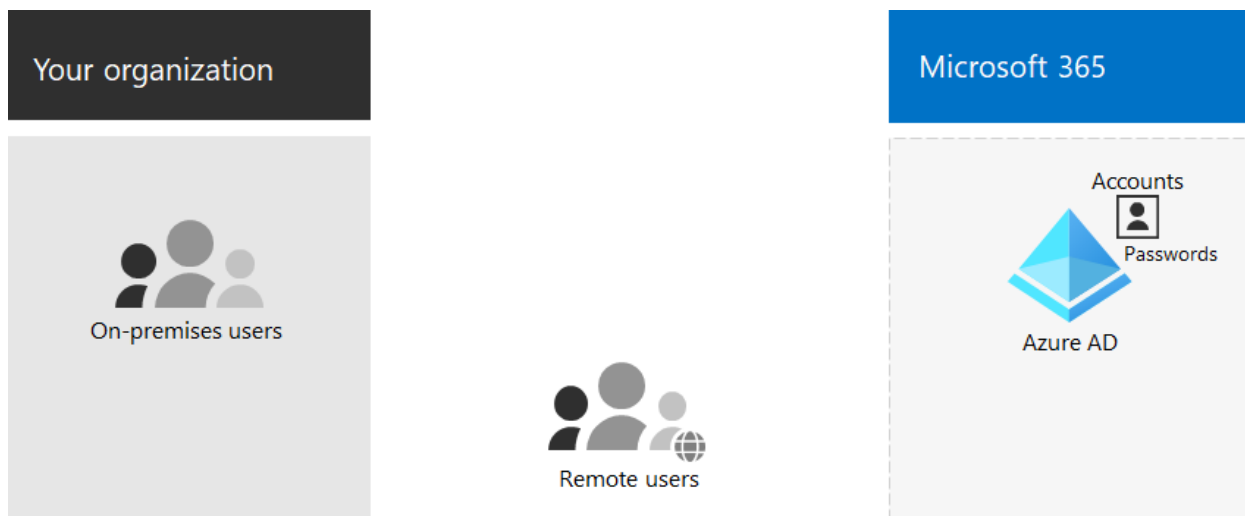
Microsoft 365 cloud-only identity

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you have chosen the cloud-only identity model, you already have an Azure Active Directory (Azure AD) tenant for your Microsoft 365 subscription to store all of your users, groups, and contacts. After setting up protection for administrator accounts in [Step 2](#) and user accounts in [Step 3](#) of this solution, you are now ready to begin creating the new accounts and groups that your organization needs.

Here are the basic components of cloud-only identity.



Users and their user accounts in organizations can be categorized in a number of ways. For example, some are employees and have a permanent status. Some are vendors, contractors, or partners that have a temporary status. Some are external users that have no user accounts but must still be granted access to specific services and resources to support interaction and collaboration. For example:

- Tenant accounts represent users within your organization that you license for cloud services
- Business to Business (B2B) accounts represent users outside your organization that you invite to participate in collaboration

Take stock of the types of users in your organization. What are the groupings? For example, you can group users by high-level function or purpose to your organization.

Additionally, some cloud services can be shared with users outside your organization without any user accounts. You'll need to identify these groups of users as well.

You can use groups in Azure AD for several purposes that simplify management of your cloud environment. For example, with Azure AD groups, you can:

- Use group-based licensing to assign licenses for Microsoft 365 to your user accounts automatically as soon as they are added as members.
- Add user accounts to specific groups dynamically based on user account attributes, such as department name.
- Automatically provision users for Software as a Service (SaaS) applications and to protect access to those applications with multi-factor authentication (MFA) and other Conditional Access policies.
- Provision permissions and levels of access for teams and SharePoint Online team sites.

Next steps for cloud-only identity

- [Manage user accounts](#)
- [Assign licenses to user accounts](#)
- [Manage groups and group membership](#)
- [Manage user account passwords](#)

Prepare for directory synchronization to Microsoft 365

10/28/2022 • 10 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you have chosen the hybrid identity model and configured protection for administrator accounts in [Step 2](#) and user accounts in [Step 3](#) of this solution, your next task is to deploy directory synchronization. The benefits of directory synchronization for your organization include:

- Reducing the administrative programs in your organization
- Optionally enabling single sign-on scenario
- Automating account changes in Microsoft 365

For more information about the advantages of using directory synchronization, see [hybrid identity with Azure Active Directory \(Azure AD\)](#).

However, directory synchronization requires planning and preparation to ensure that your Active Directory Domain Services (AD DS) synchronizes to the Azure AD tenant of your Microsoft 365 subscription with a minimum of errors.

Follow these steps in order for the best results.

NOTE

Non-ASCII characters do not sync for any attributes on the AD DS user account.

AD DS Preparation

To help ensure a seamless transition to Microsoft 365 by using synchronization, you must prepare your AD DS forest before you begin your Microsoft 365 directory synchronization deployment.

Your directory preparation should focus on the following tasks:

- Remove duplicate **proxyAddress** and **userPrincipalName** attributes.
- Update blank and invalid **userPrincipalName** attributes with valid **userPrincipalName** attributes.
- Remove invalid and questionable characters in the **givenName**, surname (**sn**), **sAMAccountName**, **displayName**, **mail**, **proxyAddresses**, **mailNickname**, and **userPrincipalName** attributes. For details about preparing attributes, see [List of attributes that are synced by the Azure Active Directory Sync Tool](#).

NOTE

These are the same attributes that Azure AD Connect synchronizes.

Multi-forest deployment considerations

For multiple forests and SSO options, use a [Custom Installation of Azure AD Connect](#).

If your organization has multiple forests for authentication (logon forests), we highly recommend the following:

- **Consider consolidating your forests.** In general, there's more overhead required to maintain multiple forests. Unless your organization has security constraints that dictate the need for separate forests, consider simplifying your on-premises environment.
- **Use only in your primary logon forest.** Consider deploying Microsoft 365 only in your primary logon forest for your initial rollout of Microsoft 365.

If you can't consolidate your multi-forest AD DS deployment or are using other directory services to manage identities, you may be able to synchronize these with the help of Microsoft or a partner.

See [Topologies for Azure AD Connect](#) for more information.

Features that are dependent on directory synchronization

Directory synchronization is required for the following features and functionality:

- Azure AD Seamless Single Sign-On (SSO)
- Skype coexistence
- Exchange hybrid deployment, including:
 - Fully shared global address list (GAL) between your on-premises Exchange environment and Microsoft 365.
 - Synchronizing GAL information from different mail systems.
 - The ability to add users to and remove users from Microsoft 365 service offerings. This requires the following:
 - Two-way synchronization must be configured during directory synchronization setup. By default, directory synchronization tools write directory information only to the cloud. When you configure two-way synchronization, you enable write-back functionality so that a limited number of object attributes are copied from the cloud, and then written them back to your local AD DS. Write-back is also referred to as Exchange hybrid mode.
 - An on-premises Exchange hybrid deployment
 - The ability to move some user mailboxes to Microsoft 365 while keeping other user mailboxes on-premises.
 - Safe senders and blocked senders on-premises are replicated to Microsoft 365.
 - Basic delegation and send-on-behalf-of email functionality.
 - You have an integrated on-premises smart card or multi-factor authentication solution.
- Synchronization of photos, thumbnails, conference rooms, and security groups

1. Directory cleanup tasks

Before you synchronize your AD DS to your Azure AD tenant, you need to clean up your AD DS.

IMPORTANT

If you don't perform AD DS cleanup before you synchronize, it can lead to a significant negative impact on the deployment process. It might take days, or even weeks, to go through the cycle of directory synchronization, identifying errors, and re-synchronization.

In your AD DS, complete the following clean-up tasks for each user account that will be assigned a Microsoft 365 license:

1. Ensure a valid and unique email address in the **proxyAddresses** attribute.
2. Remove any duplicate values in the **proxyAddresses** attribute.

3. If possible, ensure a valid and unique value for the **userPrincipalName** attribute in the user's **user** object. For the best synchronization experience, ensure that the AD DS UPN matches the Azure AD UPN. If a user doesn't have a value for the **userPrincipalName** attribute, then the **user** object must contain a valid and unique value for the **sAMAccountName** attribute. Remove any duplicate values in the **userPrincipalName** attribute.
4. For optimal use of the global address list (GAL), ensure the information in the following attributes of the AD DS user account is correct:
 - givenName
 - surname
 - displayName
 - Job Title
 - Department
 - Office
 - Office Phone
 - Mobile Phone
 - Fax Number
 - Street Address
 - City
 - State or Province
 - Zip or Postal Code
 - Country or Region

2. Directory object and attribute preparation

Successful directory synchronization between your AD DS and Microsoft 365 requires that your AD DS attributes are properly prepared. For example, you need to ensure that specific characters aren't used in certain attributes that are synchronized with the Microsoft 365 environment. Unexpected characters don't cause directory synchronization to fail but might return a warning. Invalid characters will cause directory synchronization to fail.

Directory synchronization will also fail if some of your AD DS users have one or more duplicate attributes. Each user must have unique attributes.

The attributes that you need to prepare are listed here:

- **displayName**
 - If the attribute exists in the user object, it will be synchronized with Microsoft 365.
 - If this attribute exists in the user object, there must be a value for it. That is, the attribute must not be blank.
 - Maximum number of characters: 256
- **givenName**
 - If the attribute exists in the user object, it will be synchronized with Microsoft 365, but Microsoft 365 doesn't require or use it.
 - Maximum number of characters: 64
- **mail**
 - The attribute value must be unique within the directory.

NOTE

If there are duplicate values, the first user with the value is synchronized. Subsequent users will not appear in Microsoft 365. You must modify either the value in Microsoft 365 or modify both of the values in AD DS in order for both users to appear in Microsoft 365.

- **mailNickname** (Exchange alias)

- The attribute value can't begin with a period (.).
- The attribute value must be unique within the directory.

NOTE

Underscores (" _ ") in the synchronized name indicates that the original value of this attribute contains invalid characters. For more information on this attribute, see [Exchange alias attribute](#).

- **proxyAddresses**

- Multiple-value attribute
- Maximum number of characters per value: 256
- The attribute value must not contain a space.
- The attribute value must be unique within the directory.
- Invalid characters: < > () ; , [] "
- Letters with diacritical marks, such as umlauts, accents, and tildes, are invalid characters.

The invalid characters apply to the characters following the type delimiter and ":", such that SMTP:User@contoso.com is allowed, but SMTP:user:M@contoso.com isn't.

IMPORTANT

All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards. Remove duplicate or unwanted addresses if they exist.

- **sAMAccountName**

- Maximum number of characters: 20
- The attribute value must be unique within the directory.
- Invalid characters: [\ " | , / : < > + = ; ? * ']
- If a user has an invalid **sAMAccountName** attribute but has a valid **userPrincipalName** attribute, the user account is created in Microsoft 365.
- If both **sAMAccountName** and **userPrincipalName** are invalid, the AD DS **userPrincipalName** attribute must be updated.

- **sn** (surname)

- If the attribute exists in the user object, it will be synchronized with Microsoft 365, but Microsoft 365 doesn't require or use it.

- **targetAddress**

It's required that the **targetAddress** attribute (for example, SMTP:tom@contoso.com) that's populated for the user must appear in the Microsoft 365 GAL. In third-party messaging migration scenarios, this

would require the Microsoft 365 schema extension for the AD DS. The Microsoft 365 schema extension would also add other useful attributes to manage Microsoft 365 objects that are populated by using a directory synchronization tool from AD DS. For example, the **msExchHideFromAddressLists** attribute to manage hidden mailboxes or distribution groups would be added.

- Maximum number of characters: 256
- The attribute value must not contain a space.
- The attribute value must be unique within the directory.
- Invalid characters: \ < > () ; , [] "
- All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards.

- **userPrincipalName**

- The **userPrincipalName** attribute must be in the Internet-style sign-in format where the user name is followed by the at sign (@) and a domain name: for example, user@contoso.com. All Simple Mail Transport Protocol (SMTP) addresses should comply with email messaging standards.
- The maximum number of characters for the **userPrincipalName** attribute is 113. A specific number of characters are permitted before and after the at sign (@), as follows:
- Maximum number of characters for the username that is in front of the at sign (@): 64
- Maximum number of characters for the domain name following the at sign (@): 48
- Invalid characters: \ % & * + / = ? { } | < > () ; : , [] "
- Characters allowed: A – Z, a – z, 0 – 9, ' . - _ ! # ^ ~
- Letters with diacritical marks, such as umlauts, accents, and tildes, are invalid characters.
- The @ character is required in each **userPrincipalName** value.
- The @ character can't be the first character in each **userPrincipalName** value.
- The username can't end with a period (.), an ampersand (&), a space, or an at sign (@).
- The username can't contain any spaces.
- Routable domains must be used; for example, local or internal domains can't be used.
- Unicode is converted to underscore characters.
- **userPrincipalName** can't contain any duplicate values in the directory.

3. Prepare the userPrincipalName attribute

Active Directory is designed to allow the end users in your organization to sign in to your directory by using either **sAMAccountName** or **userPrincipalName**. Similarly, end users can sign in to Microsoft 365 by using the user principal name (UPN) of their work or school account. Directory synchronization attempts to create new users in Azure Active Directory by using the same UPN that's in your AD DS. The UPN is formatted like an email address.

In Microsoft 365, the UPN is the default attribute that's used to generate the email address. It's easy to get **userPrincipalName** (in AD DS and in Azure AD) and the primary email address in **proxyAddresses** set to different values. When they're set to different values, there can be confusion for administrators and end users.

It's best to align these attributes to reduce confusion. To meet the requirements of single sign-on with Active Directory Federation Services (AD FS) 2.0, you need to ensure that the UPNs in Azure Active Directory and your AD DS match and are using a valid domain namespace.

4. Add an alternative UPN suffix to AD DS

You may need to add an alternative UPN suffix to associate the user's corporate credentials with the Microsoft 365 environment. A UPN suffix is the part of a UPN to the right of the @ character. UPNs that are used for single sign-on can contain letters, numbers, periods, dashes, and underscores, but no other types of characters.

For more information on how to add an alternative UPN suffix to Active Directory, see [Prepare for directory synchronization](#).

5. Match the AD DS UPN with the Microsoft 365 UPN

If you've already set up directory synchronization, the user's UPN for Microsoft 365 may not match the user's AD DS UPN that's defined in your AD DS. This can occur when a user was assigned a license before the domain was verified. To fix this, use [PowerShell to fix duplicate UPN](#) to update the user's UPN to ensure that the Microsoft 365 UPN matches the corporate user name and domain. If you're updating the UPN in the AD DS and would like it to synchronize with the Azure Active Directory identity, you need to remove the user's license in Microsoft 365 prior to making the changes in AD DS.

Also see [How to prepare a non-routable domain \(such as .local domain\) for directory synchronization](#).

Next steps

After you've done 1 through 5 above, see [Set up directory synchronization](#).

Prepare a non-routable domain for directory synchronization

10/28/2022 • 3 minutes to read • [Edit Online](#)

When you synchronize your on-premises directory with Microsoft 365, you have to have a verified domain in Azure Active Directory (Azure AD). Only the User Principal Names (UPNs) that are associated with the on-premises Active Directory Domain Services (AD DS) domain are synchronized. However, any UPN that contains a non-routable domain, such as ".local" (example: billa@contoso.local), will be synchronized to an .onmicrosoft.com domain (example: billa@contoso.onmicrosoft.com).

If you currently use a ".local" domain for your user accounts in AD DS, it's recommended that you change them to use a verified domain, such as billa@contoso.com, in order to properly synchronize with your Microsoft 365 domain.

What if I only have a ".local" on-premises domain?

You use Azure AD Connect for synchronizing your AD DS to the Azure AD tenant of your Microsoft 365 tenant. For more information, see [Integrating your on-premises identities with Azure AD](#).

Azure AD Connect synchronizes your users' UPN and password so that users can sign in with the same credentials they use on-premises. However, Azure AD Connect only synchronizes users to domains that are verified by Microsoft 365. This means that the domain also is verified by Azure AD because Microsoft 365 identities are managed by Azure AD. In other words, the domain has to be a valid Internet domain (such as, .com, .org, .net, .us). If your internal AD DS only uses a non-routable domain (for example, ".local"), this can't possibly match the verified domain you have for your Microsoft 365 tenant. You can fix this issue by either changing your primary domain in your on-premises AD DS, or by adding one or more UPN suffixes.

Change your primary domain

Change your primary domain to a domain you've verified in Microsoft 365, for example, contoso.com. Every user that has the domain contoso.local is then updated to contoso.com. This is an involved process, however, and an easier solution is described in the following section.

Add UPN suffixes and update your users to them

You can solve the ".local" problem by registering new UPN suffix or suffixes in AD DS to match the domain (or domains) you verified in Microsoft 365. After you register the new suffix, you update the user UPNs to replace the ".local" with the new domain name, for example, so that a user account looks like billa@contoso.com.

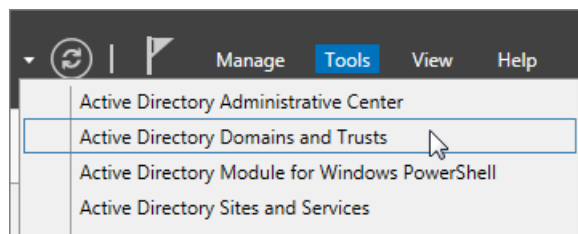
After you've updated the UPNs to use the verified domain, you're ready to synchronize your on-premises AD DS with Microsoft 365.

Step 1: Add the new UPN suffix

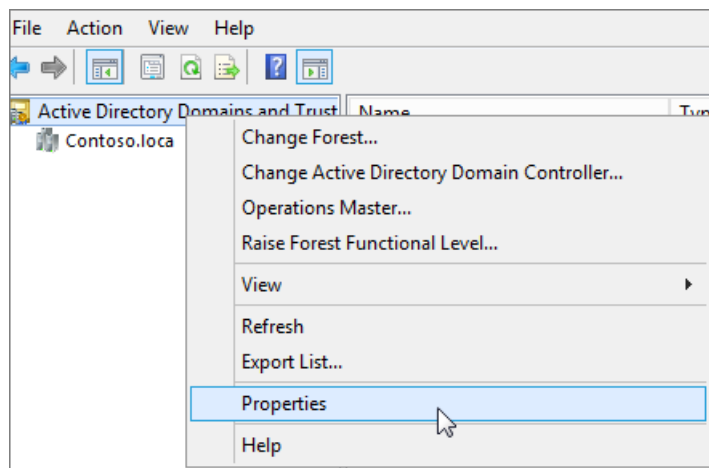
1. On the AD DS domain controller, in the Server Manager choose **Tools > Active Directory Domains and Trusts**.

Or, if you don't have Windows Server 2012

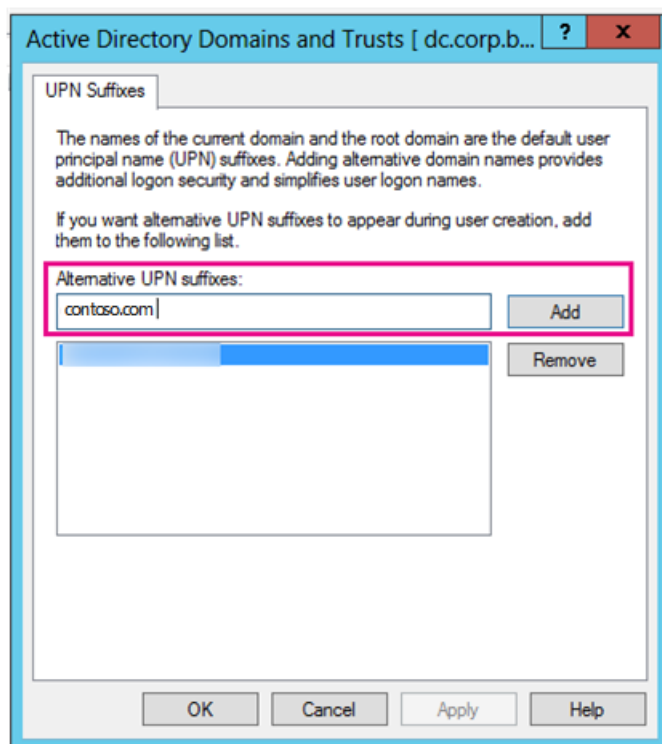
Press **Windows key + R** to open the Run dialog, and then type in Domain.msc, and then choose **OK**.



2. In the Active Directory Domains and Trusts window, right-click Active Directory Domains and Trusts, and then choose Properties.



3. On the UPN Suffixes tab, in the Alternative UPN Suffixes box, type your new UPN suffix or suffixes, and then choose Add > Apply.



Choose OK when you're done adding suffixes.

Step 2: Change the UPN suffix for existing users

1. On the AD DS domain controller, in the Server Manager choose Tools > Active Directory Users and Computers.

Or, if you don't have Windows Server 2012

Press **Windows** key + **R** to open the Run dialog, and then type in Dsa.msc, and then click **OK**

2. Select a user, right-click, and then choose **Properties**.
3. On the **Account** tab, in the UPN suffix drop-down list, choose the new UPN suffix, and then choose **OK**.

4. Complete these steps for every user.

Use PowerShell to change the UPN suffix for all of your users

If you have numerous user accounts to update, it's easier to use PowerShell. The following example uses the cmdlets [Get-ADUser](#) and [Set-ADUser](#) to change all contoso.local suffixes to contoso.com in AD DS.

For example, you could run the following PowerShell commands to update all contoso.local suffixes to contoso.com:

```
$LocalUsers = Get-ADUser -Filter "UserPrincipalName -like '*contoso.local'" -Properties userPrincipalName -
ResultSetSize $null
$LocalUsers | foreach {$newUpn = $_.UserPrincipalName.Replace("@contoso.local","@contoso.com"); $_ | Set-
ADUser -UserPrincipalName $newUpn}
```

See [Active Directory Windows PowerShell module](#) to learn more about using Windows PowerShell in AD DS.

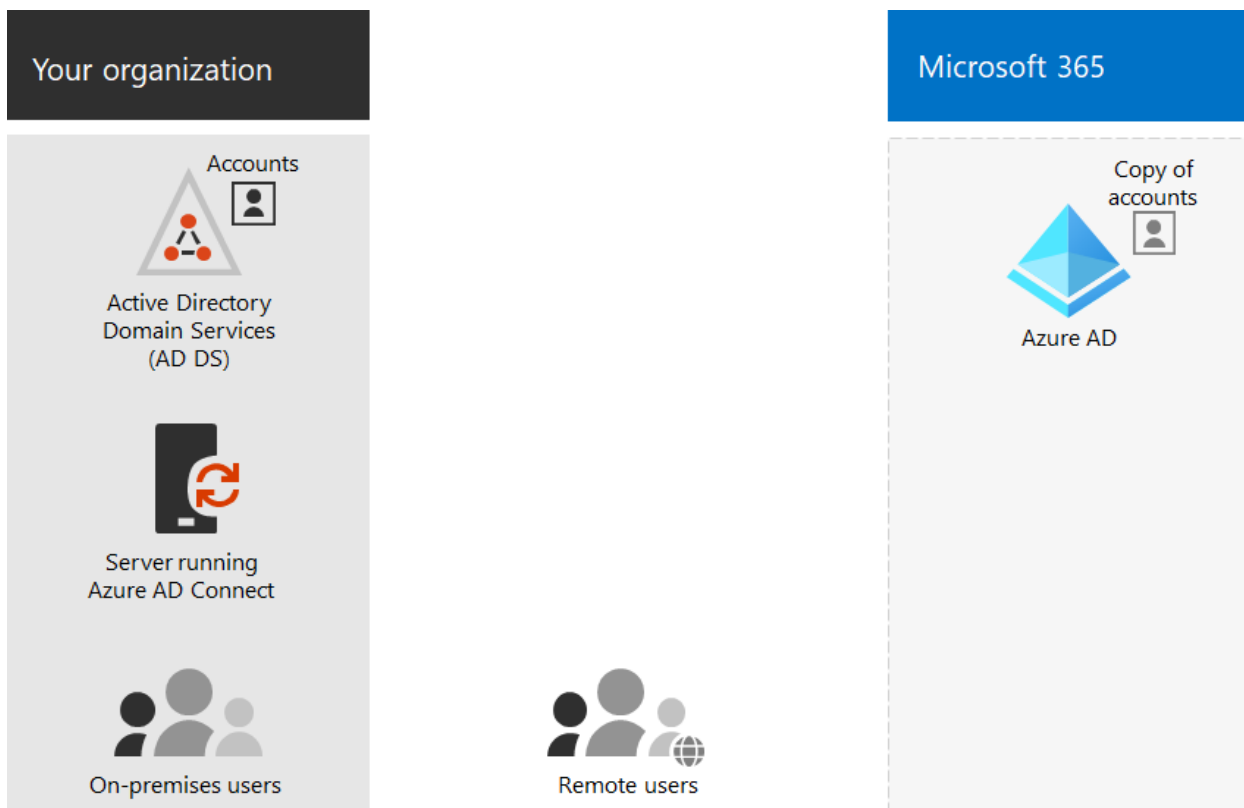
Set up directory synchronization for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 uses an Azure Active Directory (Azure AD) tenant to store and manage identities for authentication and permissions to access cloud-based resources.

If you have an on-premises Active Directory Domain Services (AD DS) domain or forest, you can synchronize your AD DS user accounts, groups, and contacts with the Azure AD tenant of your Microsoft 365 subscription. This is hybrid identity for Microsoft 365. Here are its components.



Azure AD Connect runs on an on-premises server and synchronizes your AD DS with the Azure AD tenant. Along with directory synchronization, you can also specify these authentication options:

- Password hash synchronization (PHS)

Azure AD performs the authentication itself.

- Pass-through authentication (PTA)

Azure AD has AD DS perform the authentication.

- Federated authentication

Azure AD refers the client computer requesting authentication to another identity provider.

See [Hybrid identities](#) for more information.

1. Review prerequisites for Azure AD Connect

You get a free Azure AD subscription with your Microsoft 365 subscription. When you set up directory

synchronization, you will install Azure AD Connect on one of your on-premises servers.

For Microsoft 365 you'll need to:

- Verify your on-premises domain. The Azure AD Connect wizard guides you through this.
- Obtain the user names and passwords for the admin accounts of your Microsoft 365 tenant and AD DS.

For your on-premises server on which you install Azure AD Connect, you'll need:

SERVER OS	OTHER SOFTWARE
Windows Server 2012 R2 and later	- PowerShell is installed by default, no action is required. - .Net 4.5.1 and later releases are offered through Windows Update. Make sure you have installed the latest updates to Windows Server in the Control Panel.
Windows Server 2008 R2 with Service Pack 1 (SP1)** or Windows Server 2012	- The latest version of PowerShell is available in Windows Management Framework 4.0. Search for it on Microsoft Download Center. - .Net 4.5.1 and later releases are available on Microsoft Download Center.
Windows Server 2008	- The latest supported version of PowerShell is available in Windows Management Framework 3.0, available on Microsoft Download Center. - .Net 4.5.1 and later releases are available on Microsoft Download Center.

See [Prerequisites for Azure Active Directory Connect](#) for the details of hardware, software, account and permissions requirements, SSL certificate requirements, and object limits for Azure AD Connect.

You can also review the Azure AD Connect [version release history](#) to see what is included and fixed in each release.

2. Install Azure AD Connect and configure directory synchronization

Before you begin, make sure you have:

- The user name and password of a Microsoft 365 global admin
- The user name and password of an AD DS domain administrator
- Which authentication method (PHS, PTA, federated)
- Whether you want to use [Azure AD Seamless Single Sign-on \(SSO\)](#)

Follow these steps:

1. Sign in to the [Microsoft 365 admin center](https://admin.microsoft.com) (<https://admin.microsoft.com>) and choose **Users > Active Users** on the left navigation.
2. On the **Active users** page, choose **More** (three dots) > **Directory synchronization**.
3. On the **Azure Active Directory preparation** page, select the **Go to the Download center to get the Azure AD Connect tool** link to get started.
4. Follow the steps in [Azure AD Connect and Azure AD Connect Health installation roadmap](#).

3. Finish setting up domains

Follow the steps in [Create DNS records for Microsoft 365 when you manage your DNS records](#) to finish setting up your domains.

Next step

[Assign licenses to user accounts](#)

Hybrid solutions

10/28/2022 • 2 minutes to read • [Edit Online](#)

With Microsoft Azure, you can deploy some Office Server workloads that were typically deployed on-premises in Azure infrastructure services.

For Microsoft 365 identity infrastructure in Azure:

- [Using Azure AD for SharePoint Server Authentication](#)
- [Deploy Microsoft 365 Directory Synchronization in Microsoft Azure](#)
- [Connect an on-premises network to a Microsoft Azure virtual network](#)
- [Deploy high availability federated authentication for Microsoft 365 in Azure](#)

For SharePoint Server 2013 workloads in Azure:

- [Microsoft Azure Architectures for SharePoint 2013](#)
- [SharePoint Server 2013 Disaster Recovery in Microsoft Azure](#)
- [Internet Sites in Microsoft Azure using SharePoint Server 2013](#)

Related topics

[Microsoft 365 solution and architecture center](#)

[Microsoft cloud for enterprise architects illustrations](#)

[Architectural models for SharePoint, Exchange, Skype for Business, and Lync](#)

Connect an on-premises network to a Microsoft Azure virtual network

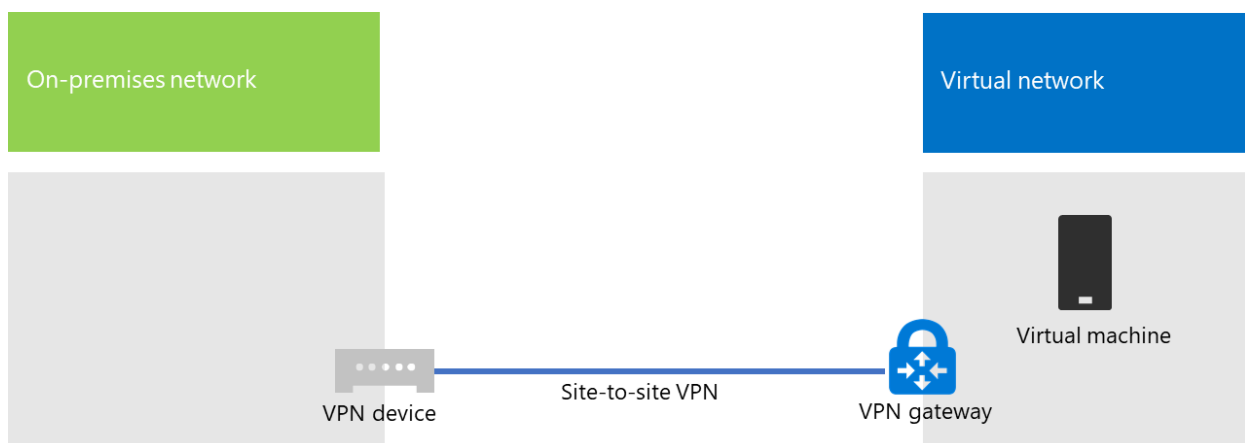
10/28/2022 • 12 minutes to read • [Edit Online](#)

A cross-premises Azure virtual network is connected to your on-premises network, extending your network to include subnets and virtual machines hosted in Azure infrastructure services. This connection lets computers on your on-premises network to directly access virtual machines in Azure and vice versa.

For example, a directory synchronization server running on an Azure virtual machine needs to query your on-premises domain controllers for changes to accounts and synchronize those changes with your Microsoft 365 subscription. This article shows you how to set up a cross-premises Azure virtual network using a site-to-site virtual private network (VPN) connection that is ready to host Azure virtual machines.

Configure a cross-premises Azure virtual network

Your virtual machines in Azure don't have to be isolated from your on-premises environment. To connect Azure virtual machines to your on-premises network resources, you must configure a cross-premises Azure virtual network. The following diagram shows the required components to deploy a cross-premises Azure virtual network with a virtual machine in Azure.



In the diagram, there are two networks connected by a site-to-site VPN connection: the on-premises network and the Azure virtual network. The site-to-site VPN connection is:

- Between two endpoints that are addressable and located on the public Internet.
- Terminated by a VPN device on the on-premises network and an Azure VPN gateway on the Azure virtual network.

The Azure virtual network hosts virtual machines. Network traffic originating from virtual machines on the Azure virtual network gets forwarded to the VPN gateway, which then forwards the traffic across the site-to-site VPN connection to the VPN device on the on-premises network. The routing infrastructure of the on-premises network then forwards the traffic to its destination.

NOTE

You can also use [ExpressRoute](#), which is a direct connection between your organization and Microsoft's network. Traffic over ExpressRoute does not travel over the public Internet. This article does not describe the use of ExpressRoute.

To set up the VPN connection between your Azure virtual network and your on-premises network, follow these

steps:

1. **On-premises:** Define and create an on-premises network route for the address space of the Azure virtual network that points to your on-premises VPN device.
2. **Microsoft Azure:** Create an Azure virtual network with a site-to-site VPN connection.
3. **On premises:** Configure your on-premises hardware or software VPN device to terminate the VPN connection, which uses Internet Protocol security (IPsec).

After you establish the site-to-site VPN connection, you add Azure virtual machines to the subnets of the virtual network.

Plan your Azure virtual network

Prerequisites

- An Azure subscription. For information about Azure subscriptions, go to the [How To Buy Azure page](#).
- An available private IPv4 address space to assign to the virtual network and its subnets, with sufficient room for growth to accommodate the number of virtual machines needed now and in the future.
- An available VPN device in your on-premises network to terminate the site-to-site VPN connection that supports the requirements for IPsec. For more information, see [About VPN devices for site-to-site virtual network connections](#).
- Changes to your routing infrastructure so that traffic routed to the address space of the Azure virtual network gets forwarded to the VPN device that hosts the site-to-site VPN connection.
- A web proxy that gives computers that are connected to the on-premises network and the Azure virtual network access to the Internet.

Solution architecture design assumptions

The following list represents the design choices that have been made for this solution architecture.

- This solution uses a single Azure virtual network with a site-to-site VPN connection. The Azure virtual network hosts a single subnet that can contain multiple virtual machines.
- You can use the Routing and Remote Access Service (RRAS) in Windows Server 2016 or Windows Server 2012 to establish an IPsec site-to-site VPN connection between the on-premises network and the Azure virtual network. You can also use other options, such as Cisco or Juniper Networks VPN devices.
- The on-premises network might still have network services like Active Directory Domain Services (AD DS), Domain Name System (DNS), and proxy servers. Depending on your requirements, it might be beneficial to place some of these network resources in the Azure virtual network.

For an existing Azure virtual network with one or more subnets, determine whether there is remaining address space for an additional subnet to host your needed virtual machines, based on your requirements. If you don't have remaining address space for an additional subnet, create an additional virtual network that has its own site-to-site VPN connection.

Plan the routing infrastructure changes for the Azure virtual network

You must configure your on-premises routing infrastructure to forward traffic destined for the address space of the Azure virtual network to the on-premises VPN device that is hosting the site-to-site VPN connection.

The exact method of updating your routing infrastructure depends on how you manage routing information, which can be:

- Routing table updates based on manual configuration.
- Routing table updates based on routing protocols, such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).

Consult with your routing specialist to make sure that traffic destined for the Azure virtual network is forwarded to the on-premises VPN device.

Plan for firewall rules for traffic to and from the on-premises VPN device

If your VPN device is on a perimeter network that has a firewall between the perimeter network and the Internet, you might have to configure the firewall for the following rules to allow the site-to-site VPN connection.

- Traffic to the VPN device (incoming from the Internet):
 - Destination IP address of the VPN device and IP protocol 50
 - Destination IP address of the VPN device and UDP destination port 500
 - Destination IP address of the VPN device and UDP destination port 4500
- Traffic from the VPN device (outgoing to the Internet):
 - Source IP address of the VPN device and IP protocol 50
 - Source IP address of the VPN device and UDP source port 500
 - Source IP address of the VPN device and UDP source port 4500

Plan for the private IP address space of the Azure virtual network

The private IP address space of the Azure virtual network must be able to accommodate addresses used by Azure to host the virtual network and with at least one subnet that has enough addresses for your Azure virtual machines.

To determine the number of addresses needed for the subnet, count the number of virtual machines that you need now, estimate for future growth, and then use the following table to determine the size of the subnet.

NUMBER OF VIRTUAL MACHINES NEEDED	NUMBER OF HOST BITS NEEDED	SIZE OF THE SUBNET
1-3	3	/29
4-11	4	/28
12-27	5	/27
28-59	6	/26
60-123	7	/25

Planning worksheet for configuring your Azure virtual network

Before you create an Azure virtual network to host virtual machines, you must determine the settings needed in the following tables.

For the settings of the virtual network, fill in Table V.

Table V: Cross-premises virtual network configuration

ITEM	CONFIGURATION ELEMENT	DESCRIPTION	VALUE
1.	Virtual network name	A name to assign to the Azure virtual network (example DirSyncNet).	_____
2.	Virtual network location	The Azure datacenter that will contain the virtual network (such as West US).	_____
3.	VPN device IP address	The public IPv4 address of your VPN device's interface on the Internet. Work with your IT department to determine this address.	_____
4.	Virtual network address space	The address space (defined in a single private address prefix) for the virtual network. Work with your IT department to determine this address space. The address space should be in Classless Interdomain Routing (CIDR) format, also known as network prefix format. An example is 10.24.64.0/20.	_____
5.	IPsec shared key	A 32-character random, alphanumeric string that will be used to authenticate both sides of the site-to-site VPN connection. Work with your IT or security department to determine this key value and then store it in a secure location. Alternately, see Create a random string for an IPsec preshared key .	_____

Fill in Table S for the subnets of this solution.

- For the first subnet, determine a 28-bit address space (with a /28 prefix length) for the Azure gateway subnet. See [Calculating the gateway subnet address space for Azure virtual networks](#) for information about how to determine this address space.
- For the second subnet, specify a friendly name, a single IP address space based on the virtual network address space, and a descriptive purpose.

Work with your IT department to determine these address spaces from the virtual network address space. Both address spaces should be in CIDR format.

Table S: Subnets in the virtual network

ITEM	SUBNET NAME	SUBNET ADDRESS SPACE	PURPOSE
------	-------------	----------------------	---------

ITEM	SUBNET NAME	SUBNET ADDRESS SPACE	PURPOSE
1.	GatewaySubnet	_____	The subnet used by the Azure gateway.
2.	_____	_____	_____

For the on-premises DNS servers that you want the virtual machines in the virtual network to use, fill in Table D. Give each DNS server a friendly name and a single IP address. This friendly name does not need to match the host name or computer name of the DNS server. Note that two blank entries are listed, but you can add more. Work with your IT department to determine this list.

Table D: On-premises DNS servers

ITEM	DNS SERVER FRIENDLY NAME	DNS SERVER IP ADDRESS
1.	_____	_____
2.	_____	_____

To route packets from the Azure virtual network to your organization network across the site-to-site VPN connection, you must configure the virtual network with a local network. This local network has a list of the address spaces (in CIDR format) for all of the locations on your organization's on-premises network that the virtual machines in the virtual network must reach. This can be all of the locations on the on-premises network or a subset. The list of address spaces that define your local network must be unique and must not overlap with the address spaces used for this virtual network or your other cross-premises virtual networks.

For the set of local network address spaces, fill in Table L. Note that three blank entries are listed but you will typically need more. Work with your IT department to determine this list.

Table L: Address prefixes for the local network

ITEM	LOCAL NETWORK ADDRESS SPACE
1.	_____
2.	_____
3.	_____

Deployment roadmap

Creating the cross-premises virtual network and adding virtual machines in Azure consists of three phases:

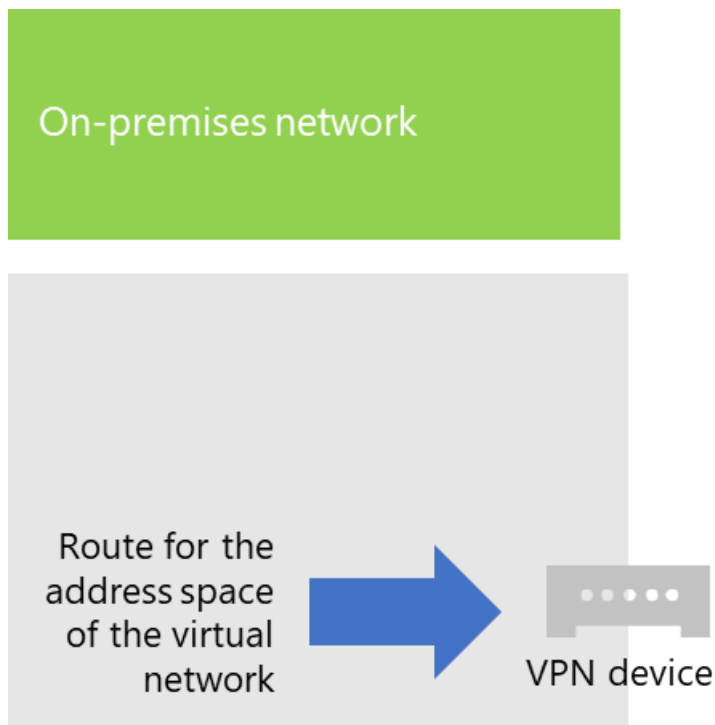
- Phase 1: Prepare your on-premises network.
- Phase 2: Create the cross-premises virtual network in Azure.
- Phase 3 (Optional): Add virtual machines.

Phase 1: Prepare your on-premises network

You must configure your on-premises network with a route that points to and ultimately delivers traffic destined

for the address space of the virtual network to the router on the edge of the on-premises network. Consult with your network administrator to determine how to add the route to the routing infrastructure of your on-premises network.

Here is your resulting configuration.



Phase 2: Create the cross-premises virtual network in Azure

First, open an Azure PowerShell prompt. If you have not installed Azure PowerShell, see [Get started with Azure PowerShell](#).

Next, login to your Azure account with this command.

```
Connect-AzAccount
```

Get your subscription name using the following command.

```
Get-AzSubscription | Sort SubscriptionName | Select SubscriptionName
```

Set your Azure subscription with these commands. Replace everything within the quotes, including the < and > characters, with the correct subscription name.

```
$subscrName="<subscription name>"  
Select-AzSubscription -SubscriptionName $subscrName
```

Next, create a new resource group for your virtual network. To determine a unique resource group name, use this command to list your existing resource groups.

```
Get-AzResourceGroup | Sort ResourceGroupName | Select ResourceGroupName
```

Create your new resource group with these commands.

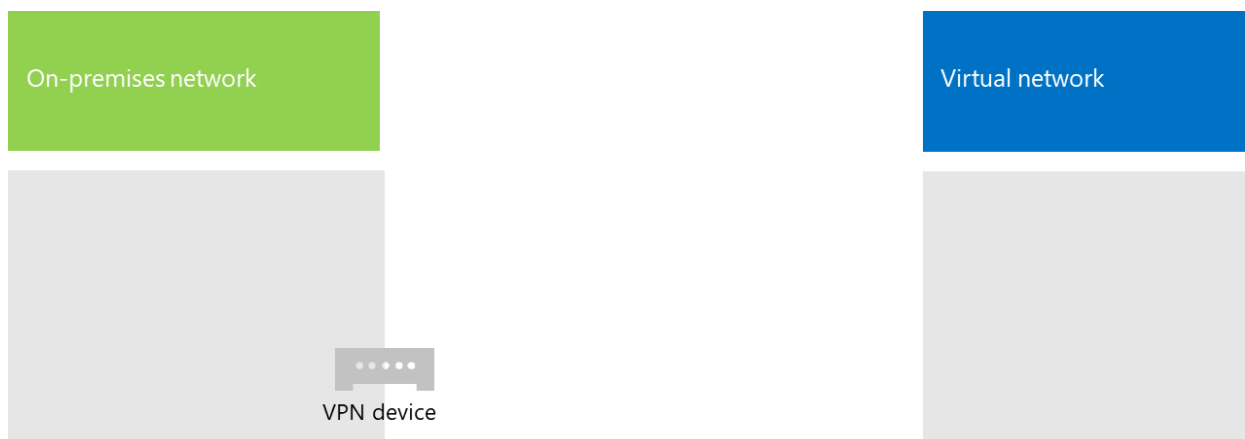
```
$rgName="<resource group name>"
$locName="<Table V - Item 2 - Value column>"
New-AzResourceGroup -Name $rgName -Location $locName
```

Next, you create the Azure virtual network.

```
# Fill in the variables from previous values and from Tables V, S, and D
$rgName="<name of your new resource group>"
$locName="<Azure location of your new resource group>"
$vnetName="<Table V - Item 1 - Value column>"
$vnetAddrPrefix="<Table V - Item 4 - Value column>"
$gwSubnetPrefix="<Table S - Item 1 - Subnet address space column>"
$SubnetName="<Table S - Item 2 - Subnet name column>"
$SubnetPrefix="<Table S - Item 2 - Subnet address space column>"
$dnsServers=@( "<Table D - Item 1 - DNS server IP address column>", "<Table D - Item 2 - DNS server IP address column>" )
$locShortName=(Get-AzResourceGroup -Name $rgName).Location

# Create the Azure virtual network and a network security group that allows incoming remote desktop connections to the subnet that is hosting virtual machines
$gatewaySubnet=New-AzVirtualNetworkSubnetConfig -Name "GatewaySubnet" -AddressPrefix $gwSubnetPrefix
$vmSubnet=New-AzVirtualNetworkSubnetConfig -Name $SubnetName -AddressPrefix $SubnetPrefix
New-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName -Location $locName -AddressPrefix $vnetAddrPrefix -Subnet $gatewaySubnet,$vmSubnet -DNSServer $dnsServers
$rule1=New-AzNetworkSecurityRuleConfig -Name "RDPTraffic" -Description "Allow RDP to all VMs on the subnet" -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389
New-AzNetworkSecurityGroup -Name $SubnetName -ResourceGroupName $rgName -Location $locShortName -SecurityRules $rule1
$vnet=Get-AzVirtualNetwork -ResourceGroupName $rgName -Name $vnetName
$nsg=Get-AzNetworkSecurityGroup -Name $SubnetName -ResourceGroupName $rgName
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name $SubnetName -AddressPrefix $SubnetPrefix -NetworkSecurityGroup $nsg
$vnet | Set-AzVirtualNetwork
```

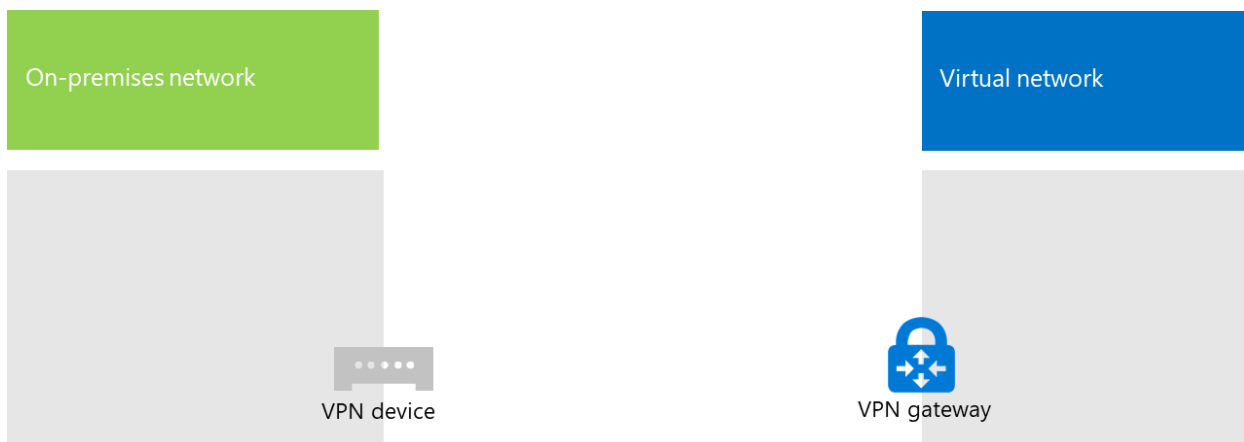
Here is your resulting configuration.



Next, use these commands to create the gateways for the site-to-site VPN connection.

```
# Fill in the variables from previous values and from Tables V and L
$vnName="Table V - Item 1 - Value column"
$localGatewayIP="Table V - Item 3 - Value column"
$localNetworkPrefix=@( <comma-separated, double-quote enclosed list of the local network address prefixes
from Table L, example: "10.1.0.0/24", "10.2.0.0/24"> )
$vnConnectionKey="Table V - Item 5 - Value column"
$vn=Get-AzVirtualNetwork -Name $vnName -ResourceGroupName $rgName
# Attach a virtual network gateway to a public IP address and the gateway subnet
$publicGatewayVipName="PublicIPAddress"
$vnGatewayIpConfigName="PublicIPConfig"
New-AzPublicIpAddress -Name $vnGatewayIpConfigName -ResourceGroupName $rgName -Location $locName -
AllocationMethod Dynamic
$publicGatewayVip=Get-AzPublicIpAddress -Name $vnGatewayIpConfigName -ResourceGroupName $rgName
$vnGatewayIpConfig=New-AzVirtualNetworkGatewayIpConfig -Name $vnGatewayIpConfigName -PublicIpAddressId
$publicGatewayVip.Id -SubnetId $vn.Subnets[0].Id
# Create the Azure gateway
$vnGatewayName="AzureGateway"
$vnGateway=New-AzVirtualNetworkGateway -Name $vnGatewayName -ResourceGroupName $rgName -Location
$locName -GatewayType Vpn -VpnType RouteBased -IpConfigurations $vnGatewayIpConfig
# Create the gateway for the local network
$localGatewayName="LocalNetGateway"
$localGateway=New-AzLocalNetworkGateway -Name $localGatewayName -ResourceGroupName $rgName -Location
$locName -GatewayIpAddress $localGatewayIP -AddressPrefix $localNetworkPrefix
# Create the Azure virtual network VPN connection
$vnConnectionName="S2SConnection"
$vnConnection=New-AzVirtualNetworkGatewayConnection -Name $vnConnectionName -ResourceGroupName $rgName -
Location $locName -ConnectionType IPsec -SharedKey $vnConnectionKey -VirtualNetworkGateway1 $vnGateway -
LocalNetworkGateway2 $localGateway
```

Here is your resulting configuration.

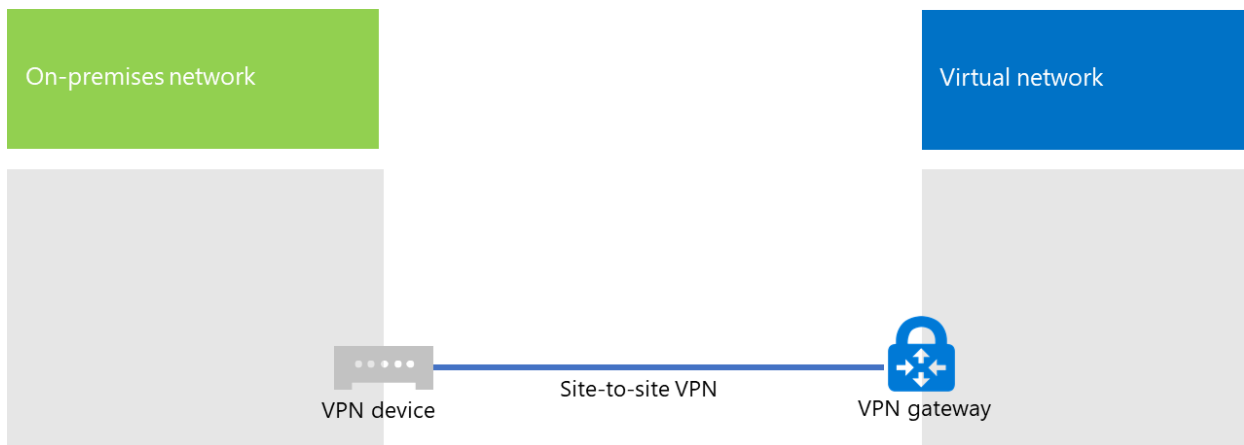


Next, configure your on-premises VPN device to connect to the Azure VPN gateway. For more information, see [About VPN Devices for site-to-site Azure Virtual Network connections](#).

To configure your VPN device, you will need the following:

- The public IPv4 address of the Azure VPN gateway for your virtual network. Use the **Get-AzPublicIpAddress -Name \$vnGatewayIpConfigName -ResourceGroupName \$rgName** command to display this address.
- The IPsec pre-shared key for the site-to-site VPN connection (Table V- Item 5 - Value column).

Here is your resulting configuration.



Phase 3 (Optional): Add virtual machines

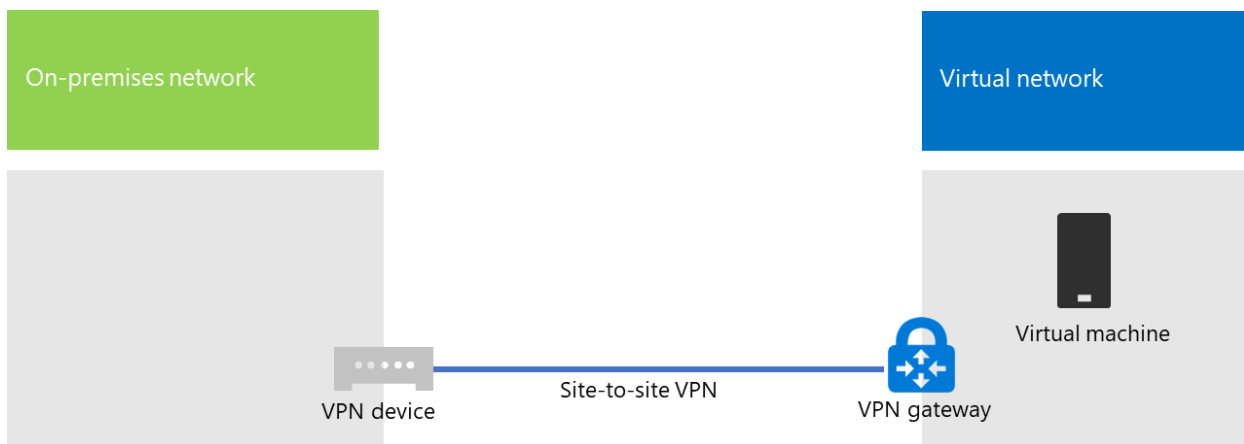
Create the virtual machines you need in Azure. For more information, see [Create a Windows virtual machine with the Azure portal](#).

Use the following settings:

- On the **Basics** tab, select the same subscription and resource group as your virtual network. You will need these later to sign in to the virtual machine. In the **Instance details** section, choose the appropriate virtual machine size. Record the administrator account user name and password in a secure location.
- On the **Networking** tab, select the name of your virtual network and the subnet for hosting virtual machines (not the GatewaySubnet). Leave all other settings at their default values.

Verify that your virtual machine is using DNS correctly by checking your internal DNS to ensure that Address (A) records were added for your new virtual machine. To access the Internet, your Azure virtual machines must be configured to use your on-premises network's proxy server. Contact your network administrator for additional configuration steps to perform on the server.

Here is your resulting configuration.



Next step

[Deploy Microsoft 365 Directory Synchronization in Microsoft Azure](#)

Deploy Microsoft 365 Directory Synchronization in Microsoft Azure

10/28/2022 • 8 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) Connect (formerly known as the Directory Synchronization tool, Directory Sync tool, or the DirSync.exe tool) is an application that you install on a domain-joined server to synchronize your on-premises Active Directory Domain Services (AD DS) users to the Azure AD tenant of your Microsoft 365 subscription. Microsoft 365 uses Azure AD for its directory service. Your Microsoft 365 subscription includes an Azure AD tenant. This tenant can also be used for management of your organization's identities with other cloud workloads, including other SaaS applications and apps in Azure.

You can install Azure AD Connect on an on-premises server, but you can also install it on a virtual machine in Azure for these reasons:

- You can provision and configure cloud-based servers faster, making the services available to your users sooner.
- Azure offers better site availability with less effort.
- You can reduce the number of on-premises servers in your organization.

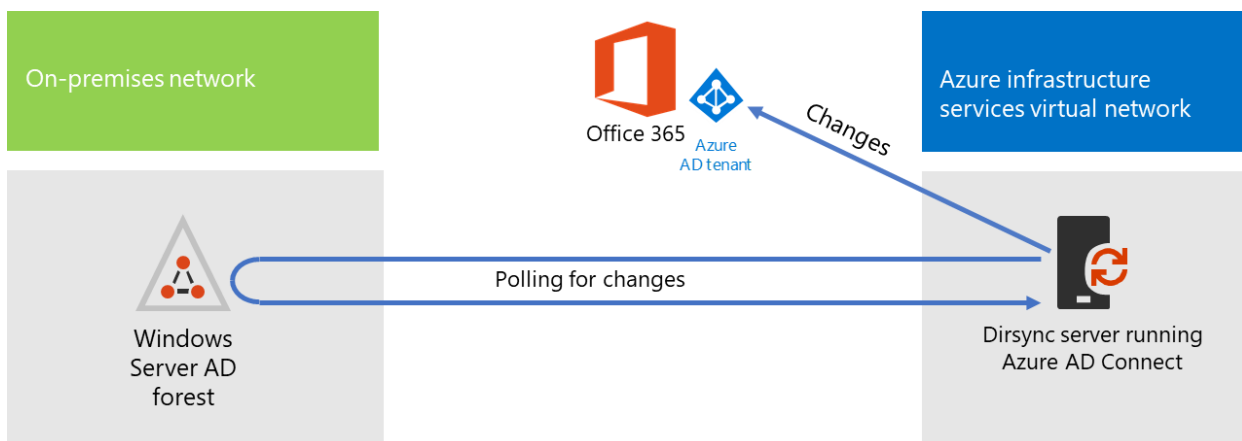
This solution requires connectivity between your on-premises network and your Azure virtual network. For more information, see [Connect an on-premises network to a Microsoft Azure virtual network](#).

NOTE

This article describes synchronization of a single domain in a single forest. Azure AD Connect synchronizes all AD DS domains in your Active Directory forest with Microsoft 365. If you have multiple Active Directory forests to synchronize with Microsoft 365, see [Multi-forest Directory Sync with Single Sign-On Scenario](#).

Overview of deploying Microsoft 365 directory synchronization in Azure

The following diagram shows Azure AD Connect running on a virtual machine in Azure (the directory sync server) that synchronizes an on-premises AD DS forest to a Microsoft 365 subscription.



In the diagram, there are two networks connected by a site-to-site VPN or ExpressRoute connection. There's an on-premises network where AD DS domain controllers are located, and there's an Azure virtual network with a directory sync server, which is a virtual machine running [Azure AD Connect](#). There are two main traffic flows

originating from the directory sync server:

- Azure AD Connect queries a domain controller on the on-premises network for changes to accounts and passwords.
- Azure AD Connect sends the changes to accounts and passwords to the Azure AD instance of your Microsoft 365 subscription. Because the directory sync server is in an extended portion of your on-premises network, these changes are sent through the on-premises network's proxy server.

NOTE

This solution describes synchronization of a single Active Directory domain, in a single Active Directory forest. Azure AD Connect synchronizes all Active Directory domains in your Active Directory forest with Microsoft 365. If you have multiple Active Directory forests to synchronize with Microsoft 365, see [Multi-forest Directory Sync with Single Sign-On Scenario](#).

There are two major steps when you deploy this solution:

1. Create an Azure virtual network and establish a site-to-site VPN connection to your on-premises network. For more information, see [Connect an on-premises network to a Microsoft Azure virtual network](#).
2. Install [Azure AD Connect](#) on a domain-joined virtual machine in Azure, and then synchronize the on-premises AD DS to Microsoft 365. This involves:

Creating an Azure Virtual Machine to run Azure AD Connect.

Installing and configuring [Azure AD Connect](#).

Configuring Azure AD Connect requires the credentials (user name and password) of an Azure AD administrator account and a AD DS enterprise administrator account. Azure AD Connect runs immediately and on an ongoing basis to synchronize the on-premises AD DS forest to Microsoft 365.

Before you deploy this solution in production, you can use the instructions in [The simulated enterprise base configuration](#) to set up this configuration as a proof of concept, for demonstrations, or for experimentation.

IMPORTANT

When Azure AD Connect configuration completes, it does not save the AD DS enterprise administrator account credentials.

NOTE

This solution describes synchronizing a single AD DS forest to Microsoft 365. The topology discussed in this article represents only one way to implement this solution. Your organization's topology might differ based on your unique network requirements and security considerations.

Plan for hosting a directory sync server for Microsoft 365 in Azure

Prerequisites

Before you begin, review the following prerequisites for this solution:

- Review the related planning content in [Plan your Azure virtual network](#).
- Ensure that you meet all [Prerequisites](#) for configuring the Azure virtual network.
- Have a Microsoft 365 subscription that includes the Active Directory integration feature. For information

about Microsoft 365 subscriptions, go to the [Microsoft 365 subscription page](#).

- Provision one Azure Virtual Machine that runs Azure AD Connect to synchronize your on-premises AD DS forest with Microsoft 365.

You must have the credentials (names and passwords) for a AD DS enterprise administrator account and an Azure AD Administrator account.

Solution architecture design assumptions

The following list describes the design choices made for this solution.

- This solution uses a single Azure virtual network with a site-to-site VPN connection. The Azure virtual network hosts a single subnet that has one server, the directory sync server that is running Azure AD Connect.
- On the on-premises network, a domain controller and DNS servers exist.
- Azure AD Connect performs password hash synchronization instead of single sign-on. You don't have to deploy an Active Directory Federation Services (AD FS) infrastructure. To learn more about password hash synchronization and single sign-on options, see [Choosing the right authentication method for your Azure Active Directory hybrid identity solution](#).

There are other design choices that you might consider when you deploy this solution in your environment. These include the following:

- If there are existing DNS servers in an existing Azure virtual network, determine whether you want your directory sync server to use them for name resolution instead of DNS servers on the on-premises network.
- If there are domain controllers in an existing Azure virtual network, determine whether configuring Active Directory Sites and Services may be a better option for you. The directory sync server can query the domain controllers in the Azure virtual network for changes in accounts and passwords instead of domain controllers on the on-premises network.

Deployment roadmap

Deploying Azure AD Connect on a virtual machine in Azure consists of three phases:

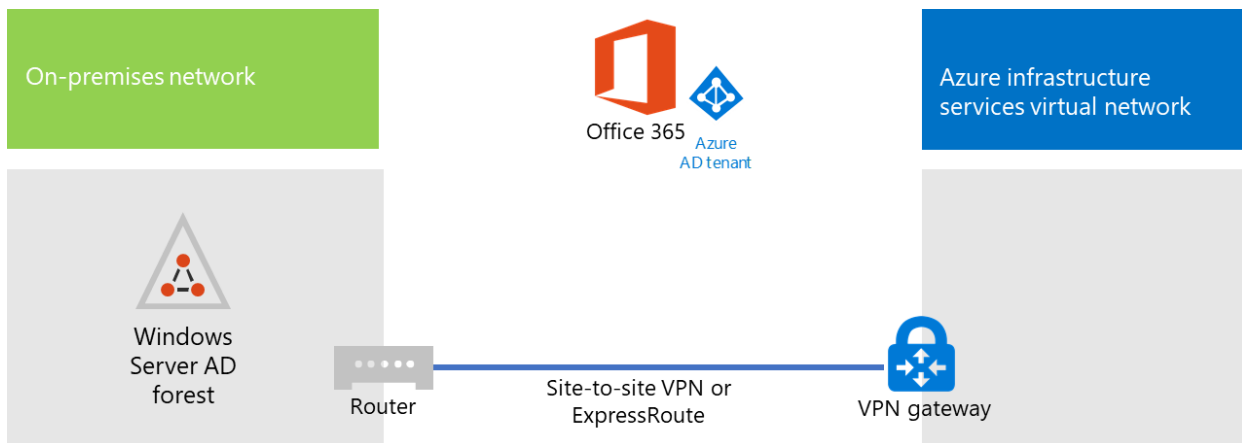
- Phase 1: Create and configure the Azure virtual network
- Phase 2: Create and configure the Azure virtual machine
- Phase 3: Install and configure Azure AD Connect

After deployment, you must also assign locations and licenses for the new user accounts in Microsoft 365.

Phase 1: Create and configure the Azure virtual network

To create and configure the Azure virtual network, complete [Phase 1: Prepare your on-premises network](#) and [Phase 2: Create the cross-premises virtual network in Azure](#) in the deployment roadmap of [Connect an on-premises network to a Microsoft Azure virtual network](#).

This is your resulting configuration.



This figure shows an on-premises network connected to an Azure virtual network through a site-to-site VPN or ExpressRoute connection.

Phase 2: Create and configure the Azure virtual machine

Create the virtual machine in Azure using the instructions [Create your first Windows virtual machine in the Azure portal](#). Use the following settings:

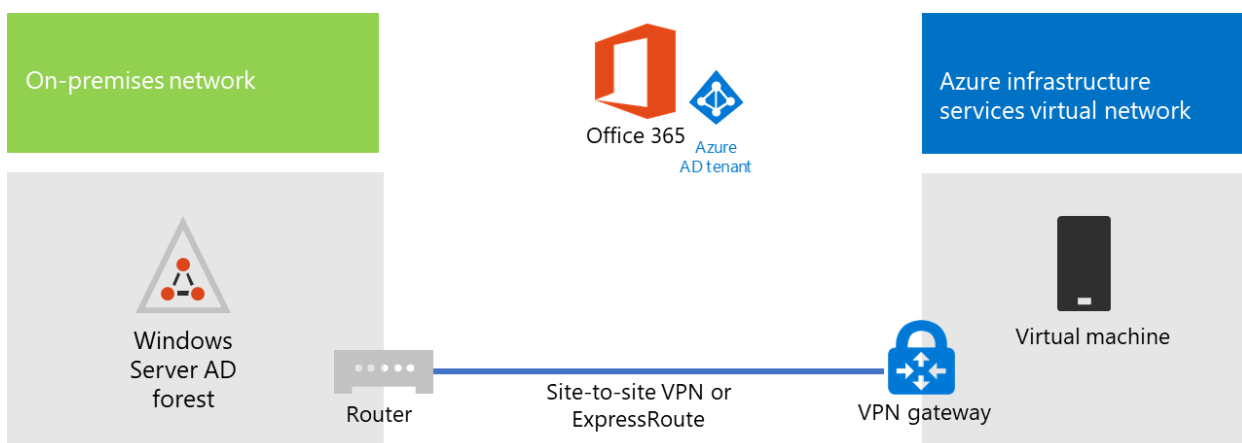
- On the **Basics** pane, select the same subscription, location, and resource group as your virtual network. Record the user name and password in a secure location. You will need these later to connect to the virtual machine.
- On the **Choose a size** pane, choose the **A2 Standard** size.
- On the **Settings** pane, in the **Storage** section, select the **Standard** storage type. In the **Network** section, select the name of your virtual network and the subnet for hosting the directory sync server (not the GatewaySubnet). Leave all other settings at their default values.

Verify that your directory sync server is using DNS correctly by checking your internal DNS to make sure that an Address (A) record was added for the virtual machine with its IP address.

Use the instructions in [Connect to the virtual machine and sign on](#) to connect to the directory sync server with a Remote Desktop Connection. After signing in, join the virtual machine to the on-premises AD DS domain.

For Azure AD Connect to gain access to Internet resources, you must configure the directory sync server to use the on-premises network's proxy server. You should contact your network administrator for any additional configuration steps to perform.

This is your resulting configuration.



This figure shows the directory sync server virtual machine in the cross-premises Azure virtual network.

Phase 3: Install and configure Azure AD Connect

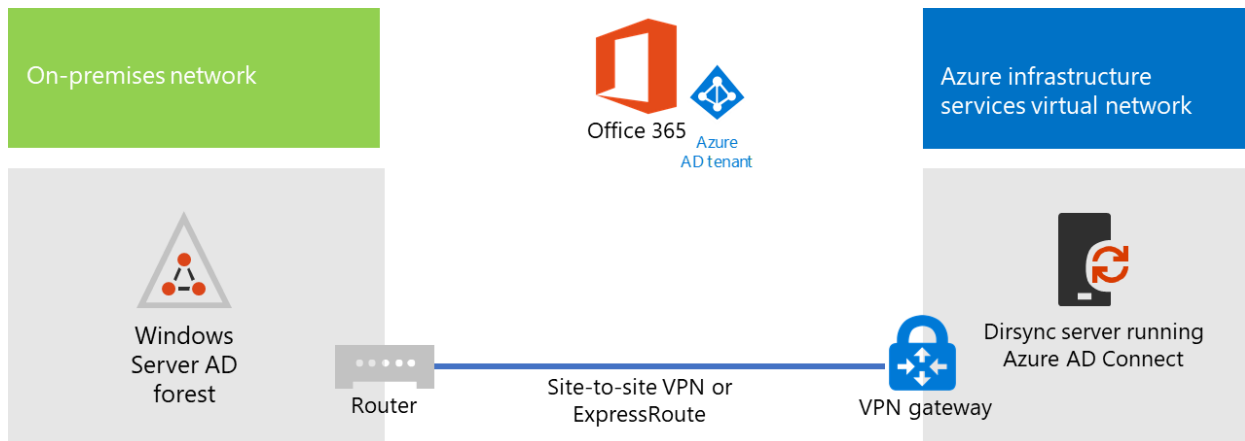
Complete the following procedure:

1. Connect to the directory sync server using a Remote Desktop Connection with an AD DS domain account that has local administrator privileges. See [Connect to the virtual machine and sign on](#).
2. From the directory sync server, open the [Set up directory synchronization for Microsoft 365](#) article and follow the directions for directory synchronization with password hash synchronization.

Caution

Setup creates the `AAD_XXXXXXXXXX` account in the Local Users organizational unit (OU). Do not move or remove this account or synchronization will fail.

This is your resulting configuration.



This figure shows the directory sync server with Azure AD Connect in the cross-premises Azure virtual network.

Assign locations and licenses to users in Microsoft 365

Azure AD Connect adds accounts to your Microsoft 365 subscription from the on-premises AD DS, but in order for users to sign in to Microsoft 365 and use its services, the accounts must be configured with a location and licenses. Use these steps to add the location and activate licenses for the appropriate user accounts:

1. Sign in to the [Microsoft 365 admin center](#), and then click **Admin**.
2. In the left navigation, click **Users** > [Active users](#).
3. In the list of user accounts, select the check box next to the user you want to activate.
4. On the page for the user, click **Edit** for **Product licenses**.
5. On the **Product licenses** page, select a location for the user for **Location**, and then enable the appropriate licenses for the user.
6. When complete, click **Save**, and then click **Close** twice.
7. Go back to step 3 for additional users.

See also

[Microsoft 365 solution and architecture center](#)

[Connect an on-premises network to a Microsoft Azure virtual network](#)

[Download Azure AD Connect](#)

[Set up directory synchronization for Microsoft 365](#)

Deploy high availability federated authentication for Microsoft 365 in Azure

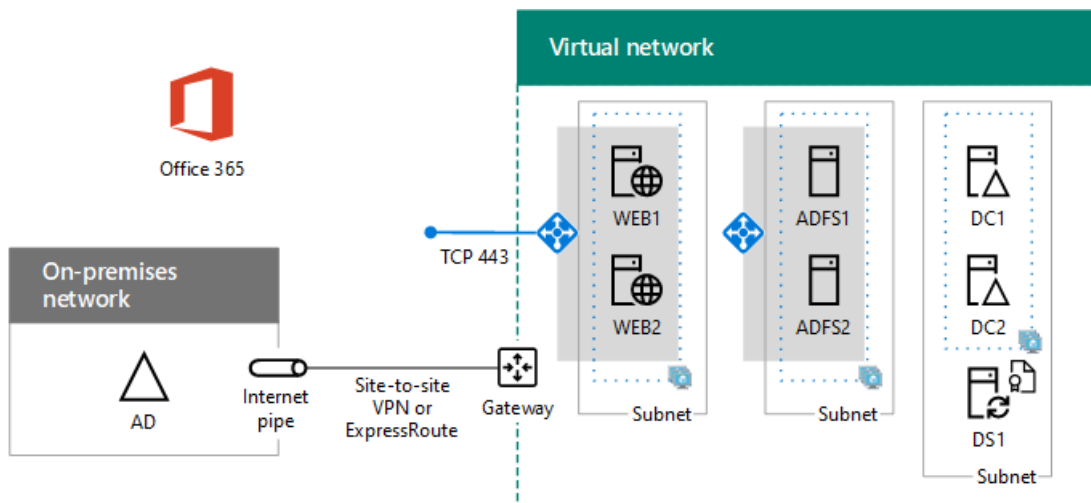
10/28/2022 • 3 minutes to read • [Edit Online](#)

This article has links to the step-by-step instructions for deploying high availability federated authentication for Microsoft Microsoft 365 in Azure infrastructure services with these virtual machines:

- Two web application proxy servers
- Two Active Directory Federation Services (AD FS) servers
- Two replica domain controllers
- One directory synchronization server running Azure AD Connect

Here is the configuration, with placeholder names for each server.

A high availability federated authentication for Microsoft 365 infrastructure in Azure



All of the virtual machines are in a single cross-premises Azure virtual network (VNet).

NOTE

Federated authentication of individual users does not rely on any on-premises resources. However, if the cross-premises connection becomes unavailable, the domain controllers in the VNet will not receive updates to user accounts and groups made in the on-premises Active Directory Domain Services (AD DS). To ensure this does not happen, you can configure high availability for your cross-premises connection. For more information, see [Highly Available Cross-Premises and VNet-to-VNet Connectivity](#)

Each pair of virtual machines for a specific role is in its own subnet and availability set.

NOTE

Because this VNet is connected to the on-premises network, this configuration does not include jumpbox or monitoring virtual machines on a management subnet. For more information, see [Running Windows VMs for an N-tier architecture](#).

The result of this configuration is that you will have federated authentication for all of your Microsoft 365 users,

in which they can use their AD DS credentials to sign in rather than their Microsoft 365 account. The federated authentication infrastructure uses a redundant set of servers that are more easily deployed in Azure infrastructure services, rather than in your on-premises edge network.

Bill of materials

This baseline configuration requires the following set of Azure services and components:

- Seven virtual machines
- One cross-premises virtual network with four subnets
- Four resource groups
- Three availability sets
- One Azure subscription

Here are the virtual machines and their default sizes for this configuration.

ITEM	VIRTUAL MACHINE DESCRIPTION	AZURE GALLERY IMAGE	DEFAULT SIZE
1.	First domain controller	Windows Server 2016 Datacenter	D2
2.	Second domain controller	Windows Server 2016 Datacenter	D2
3.	Azure AD Connect server	Windows Server 2016 Datacenter	D2
4.	First AD FS server	Windows Server 2016 Datacenter	D2
5.	Second AD FS server	Windows Server 2016 Datacenter	D2
6.	First web application proxy server	Windows Server 2016 Datacenter	D2
7.	Second web application proxy server	Windows Server 2016 Datacenter	D2

To compute the estimated costs for this configuration, see the [Azure pricing calculator](#)

Phases of deployment

You deploy this workload in the following phases:

- [Phase 1: Configure Azure](#). Create resource groups, storage accounts, availability sets, and a cross-premises virtual network.
- [Phase 2: Configure domain controllers](#). Create and configure replica AD DS domain controllers and the directory synchronization server.
- [Phase 3: Configure AD FS servers](#). Create and configure the two AD FS servers.
- [Phase 4: Configure web application proxies](#). Create and configure the two web application proxy servers.

- [Phase 5: Configure federated authentication for Microsoft 365](#). Configure federated authentication for your Microsoft 365 subscription.

These articles provide a prescriptive, phase-by-phase guide for a predefined architecture to create a functional, high availability federated authentication for Microsoft 365 in Azure infrastructure services. Keep the following in mind:

- If you are an experienced AD FS implementer, feel free to adapt the instructions in phases 3 and 4 and build the set of servers that best suits your needs.
- If you already have an existing Azure hybrid cloud deployment with an existing cross-premises virtual network, feel free to adapt or skip the instructions in phases 1 and 2 and place the AD FS and web application proxy servers on the appropriate subnets.

To build a dev/test environment or a proof-of-concept of this configuration, see [Federated identity for your Microsoft 365 dev/test environment](#).

Next step

Start the configuration of this workload with [Phase 1: Configure Azure](#).

High availability federated authentication Phase 1: Configure Azure

10/28/2022 • 10 minutes to read • [Edit Online](#)

In this phase, you create the resource groups, virtual network (VNet), and availability sets in Azure that will host the virtual machines in phases 2, 3, and 4. You must complete this phase before moving on to [Phase 2: Configure domain controllers](#). See [Deploy high availability federated authentication for Microsoft 365 in Azure](#) for all of the phases.

Azure must be provisioned with these basic components:

- Resource groups
- A cross-premises Azure virtual network (VNet) with subnets for hosting the Azure virtual machines
- Network security groups for performing subnet isolation
- Availability sets

Configure Azure components

Before you begin configuring Azure components, fill in the following tables. To assist you in the procedures for configuring Azure, print this section and write down the needed information or copy this section to a document and fill it in. For the settings of the VNet, fill in Table V.

ITEM	CONFIGURATION SETTING	DESCRIPTION	VALUE
1.	VNet name	A name to assign to the VNet (example FedAuthNet).	_____
2.	VNet location	The regional Azure datacenter that will contain the virtual network.	_____
3.	VPN device IP address	The public IPv4 address of your VPN device's interface on the Internet.	_____
4.	VNet address space	The address space for the virtual network. Work with your IT department to determine this address space.	_____

ITEM	CONFIGURATION SETTING	DESCRIPTION	VALUE
5.	IPsec shared key	A 32-character random, alphanumeric string that will be used to authenticate both sides of the site-to-site VPN connection. Work with your IT or security department to determine this key value. Alternately, see Create a random string for an IPsec preshared key .	_____

Table V: Cross-premises virtual network configuration

Next, fill in Table S for the subnets of this solution. All address spaces should be in Classless Interdomain Routing (CIDR) format, also known as network prefix format. An example is 10.24.64.0/20.

For the first three subnets, specify a name and a single IP address space based on the virtual network address space. For the gateway subnet, determine the 27-bit address space (with a /27 prefix length) for the Azure gateway subnet with the following:

1. Set the variable bits in the address space of the VNet to 1, up to the bits being used by the gateway subnet, then set the remaining bits to 0.
2. Convert the resulting bits to decimal and express it as an address space with the prefix length set to the size of the gateway subnet.

See [Address space calculator for Azure gateway subnets](#) for a PowerShell command block and C# or Python console application that performs this calculation for you.

Work with your IT department to determine these address spaces from the virtual network address space.

ITEM	SUBNET NAME	SUBNET ADDRESS SPACE	PURPOSE
1.	_____	_____	The subnet used by the Active Directory Domain Services (AD DS) domain controller and directory synchronization server virtual machines (VMs).
2.	_____	_____	The subnet used by the AD FS VMs.
3.	_____	_____	The subnet used by the web application proxy VMs.
4.	GatewaySubnet	_____	The subnet used by the Azure gateway VMs.

Table S: Subnets in the virtual network

Next, fill in Table I for the static IP addresses assigned to virtual machines and load balancer instances.

ITEM	PURPOSE	IP ADDRESS ON THE SUBNET	VALUE
------	---------	--------------------------	-------

ITEM	PURPOSE	IP ADDRESS ON THE SUBNET	VALUE
1.	Static IP address of the first domain controller	The fourth possible IP address for the address space of the subnet defined in Item 1 of Table S.	_____
2.	Static IP address of the second domain controller	The fifth possible IP address for the address space of the subnet defined in Item 1 of Table S.	_____
3.	Static IP address of the directory synchronization server	The sixth possible IP address for the address space of the subnet defined in Item 1 of Table S.	_____
4.	Static IP address of the internal load balancer for the AD FS servers	The fourth possible IP address for the address space of the subnet defined in Item 2 of Table S.	_____
5.	Static IP address of the first AD FS server	The fifth possible IP address for the address space of the subnet defined in Item 2 of Table S.	_____
6.	Static IP address of the second AD FS server	The sixth possible IP address for the address space of the subnet defined in Item 2 of Table S.	_____
7.	Static IP address of the first web application proxy server	The fourth possible IP address for the address space of the subnet defined in Item 3 of Table S.	_____
8.	Static IP address of the second web application proxy server	The fifth possible IP address for the address space of the subnet defined in Item 3 of Table S.	_____

Table I: Static IP addresses in the virtual network

For two Domain Name System (DNS) servers in your on-premises network that you want to use when initially setting up the domain controllers in your virtual network, fill in Table D. Work with your IT department to determine this list.

ITEM	DNS SERVER FRIENDLY NAME	DNS SERVER IP ADDRESS
1.	_____	_____
2.	_____	_____

Table D: On-premises DNS servers

To route packets from the cross-premises network to your organization network across the site-to-site VPN

connection, you must configure the virtual network with a local network that has a list of the address spaces (in CIDR notation) for all of the reachable locations on your organization's on-premises network. The list of address spaces that define your local network must be unique and must not overlap with the address space used for other virtual networks or other local networks.

For the set of local network address spaces, fill in Table L. Note that three blank entries are listed but you will typically need more. Work with your IT department to determine this list of address spaces.

ITEM	LOCAL NETWORK ADDRESS SPACE
1.	_____
2.	_____
3.	_____

Table L: Address prefixes for the local network

Now let's begin building the Azure infrastructure to host your federated authentication for Microsoft 365.

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell](#).

First, start an Azure PowerShell prompt and login to your account.

```
Connect-AzAccount
```

TIP

To generate ready-to-run PowerShell command blocks based on your custom settings, use this [Microsoft Excel configuration workbook](#).

Get your subscription name using the following command.

```
Get-AzSubscription | Sort Name | Select Name
```

For older versions of Azure PowerShell, use this command instead.

```
Get-AzSubscription | Sort Name | Select SubscriptionName
```

Set your Azure subscription. Replace everything within the quotes, including the < and > characters, with the correct name.

```
$subscrName="<subscription name>"  
Select-AzSubscription -SubscriptionName $subscrName
```

Next, create the new resource groups. To determine a unique set of resource group names, use this command to list your existing resource groups.

Fill in the following table for the set of unique resource group names.

ITEM	RESOURCE GROUP NAME	PURPOSE
1.	_____	Domain controllers
2.	_____	AD FS servers
3.	_____	Web application proxy servers
4.	_____	Infrastructure elements

Table R: Resource groups

Create your new resource groups with these commands.

```
$locName="<an Azure location, such as West US>"
$rgName="<Table R - Item 1 - Name column>"
New-AzResourceGroup -Name $rgName -Location $locName
$rgName="<Table R - Item 2 - Name column>"
New-AzResourceGroup -Name $rgName -Location $locName
$rgName="<Table R - Item 3 - Name column>"
New-AzResourceGroup -Name $rgName -Location $locName
$rgName="<Table R - Item 4 - Name column>"
New-AzResourceGroup -Name $rgName -Location $locName
```

Next, you create the Azure virtual network and its subnets.

```
$rgName="<Table R - Item 4 - Resource group name column>"
$locName="<your Azure location>"
$vnetName="<Table V - Item 1 - Value column>"
$vnetAddrPrefix="<Table V - Item 4 - Value column>"
$dnsServers=@( "<Table D - Item 1 - DNS server IP address column>", "<Table D - Item 2 - DNS server IP address column>" )
# Get the shortened version of the location
$locShortName=(Get-AzResourceGroup -Name $rgName).Location

# Create the subnets
$subnet1Name="<Table S - Item 1 - Subnet name column>"
$subnet1Prefix="<Table S - Item 1 - Subnet address space column>"
$subnet1=New-AzVirtualNetworkSubnetConfig -Name $subnet1Name -AddressPrefix $subnet1Prefix
$subnet2Name="<Table S - Item 2 - Subnet name column>"
$subnet2Prefix="<Table S - Item 2 - Subnet address space column>"
$subnet2=New-AzVirtualNetworkSubnetConfig -Name $subnet2Name -AddressPrefix $subnet2Prefix
$subnet3Name="<Table S - Item 3 - Subnet name column>"
$subnet3Prefix="<Table S - Item 3 - Subnet address space column>"
$subnet3=New-AzVirtualNetworkSubnetConfig -Name $subnet3Name -AddressPrefix $subnet3Prefix
$gwSubnet4Prefix="<Table S - Item 4 - Subnet address space column>"
$gwSubnet=New-AzVirtualNetworkSubnetConfig -Name "GatewaySubnet" -AddressPrefix $gwSubnet4Prefix

# Create the virtual network
New-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName -Location $locName -AddressPrefix $vnetAddrPrefix -Subnet $gwSubnet,$subnet1,$subnet2,$subnet3 -DNSServer $dnsServers
```

Next, you create network security groups for each subnet that has virtual machines. To perform subnet isolation,

you can add rules for the specific types of traffic allowed or denied to the network security group of a subnet.

```
# Create network security groups
$vnnet=Get-AzVirtualNetwork -ResourceGroupName $rgName -Name $vnnetName

New-AzNetworkSecurityGroup -Name $subnet1Name -ResourceGroupName $rgName -Location $locShortName
$nsg=Get-AzNetworkSecurityGroup -Name $subnet1Name -ResourceGroupName $rgName
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnnet -Name $subnet1Name -AddressPrefix $subnet1Prefix -
NetworkSecurityGroup $nsg

New-AzNetworkSecurityGroup -Name $subnet2Name -ResourceGroupName $rgName -Location $locShortName
$nsg=Get-AzNetworkSecurityGroup -Name $subnet2Name -ResourceGroupName $rgName
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnnet -Name $subnet2Name -AddressPrefix $subnet2Prefix -
NetworkSecurityGroup $nsg

New-AzNetworkSecurityGroup -Name $subnet3Name -ResourceGroupName $rgName -Location $locShortName
$nsg=Get-AzNetworkSecurityGroup -Name $subnet3Name -ResourceGroupName $rgName
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnnet -Name $subnet3Name -AddressPrefix $subnet3Prefix -
NetworkSecurityGroup $nsg
$vnnet | Set-AzVirtualNetwork
```

Next, use these commands to create the gateways for the site-to-site VPN connection.

```
$rgName="<Table R - Item 4 - Resource group name column>"
$locName="<Azure location>"
$vnnetName="<Table V - Item 1 - Value column>"
$vnnet=Get-AzVirtualNetwork -Name $vnnetName -ResourceGroupName $rgName
$subnet=Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnnet -Name "GatewaySubnet"

# Attach a virtual network gateway to a public IP address and the gateway subnet
$publicGatewayVipName="PublicIPAddress"
$vnnetGatewayIpConfigName="PublicIPConfig"
New-AzPublicIpAddress -Name $vnnetGatewayIpConfigName -ResourceGroupName $rgName -Location $locName -
AllocationMethod Dynamic
$publicGatewayVip=Get-AzPublicIpAddress -Name $vnnetGatewayIpConfigName -ResourceGroupName $rgName
$vnnetGatewayIpConfig=New-AzVirtualNetworkGatewayIpConfig -Name $vnnetGatewayIpConfigName -PublicIpAddressId
$publicGatewayVip.Id -Subnet $subnet

# Create the Azure gateway
$vnnetGatewayName="AzureGateway"
$vnnetGateway=New-AzVirtualNetworkGateway -Name $vnnetGatewayName -ResourceGroupName $rgName -Location
$locName -GatewayType Vpn -VpnType RouteBased -IpConfigurations $vnnetGatewayIpConfig

# Create the gateway for the local network
$localGatewayName="LocalNetGateway"
$localGatewayIP="<Table V - Item 3 - Value column>"
$localNetworkPrefix=@( <comma-separated, double-quote enclosed list of the local network address prefixes
from Table L, example: "10.1.0.0/24", "10.2.0.0/24"> )
$localGateway=New-AzLocalNetworkGateway -Name $localGatewayName -ResourceGroupName $rgName -Location
$locName -GatewayIpAddress $localGatewayIP -AddressPrefix $localNetworkPrefix

# Define the Azure virtual network VPN connection
$vnnetConnectionName="S2SConnection"
$vnnetConnectionKey="<Table V - Item 5 - Value column>"
$vnnetConnection=New-AzVirtualNetworkGatewayConnection -Name $vnnetConnectionName -ResourceGroupName $rgName -
Location $locName -ConnectionType IPsec -SharedKey $vnnetConnectionKey -VirtualNetworkGateway1 $vnnetGateway -
LocalNetworkGateway2 $localGateway
```

NOTE

Federated authentication of individual users does not rely on any on-premises resources. However, if this site-to-site VPN connection becomes unavailable, the domain controllers in the VNet will not receive updates to user accounts and groups made in the on-premises Active Directory Domain Services. To ensure this does not happen, you can configure high availability for your site-to-site VPN connection. For more information, see [Highly Available Cross-Premises and VNet-to-VNet Connectivity](#)

Next, record the public IPv4 address of the Azure VPN gateway for your virtual network from the display of this command:

```
Get-AzPublicIpAddress -Name $publicGatewayVipName -ResourceGroupName $rgName
```

Next, configure your on-premises VPN device to connect to the Azure VPN gateway. For more information, see [Configure your VPN device](#).

To configure your on-premises VPN device, you will need the following:

- The public IPv4 address of the Azure VPN gateway.
- The IPsec pre-shared key for the site-to-site VPN connection (Table V - Item 5 - Value column).

Next, ensure that the address space of the virtual network is reachable from your on-premises network. This is usually done by adding a route corresponding to the virtual network address space to your VPN device and then advertising that route to the rest of the routing infrastructure of your organization network. Work with your IT department to determine how to do this.

Next, define the names of three availability sets. Fill out Table A.

ITEM	PURPOSE	AVAILABILITY SET NAME
1.	Domain controllers	_____
2.	AD FS servers	_____
3.	Web application proxy servers	_____

Table A: Availability sets

You will need these names when you create the virtual machines in phases 2, 3, and 4.

Create the new availability sets with these Azure PowerShell commands.

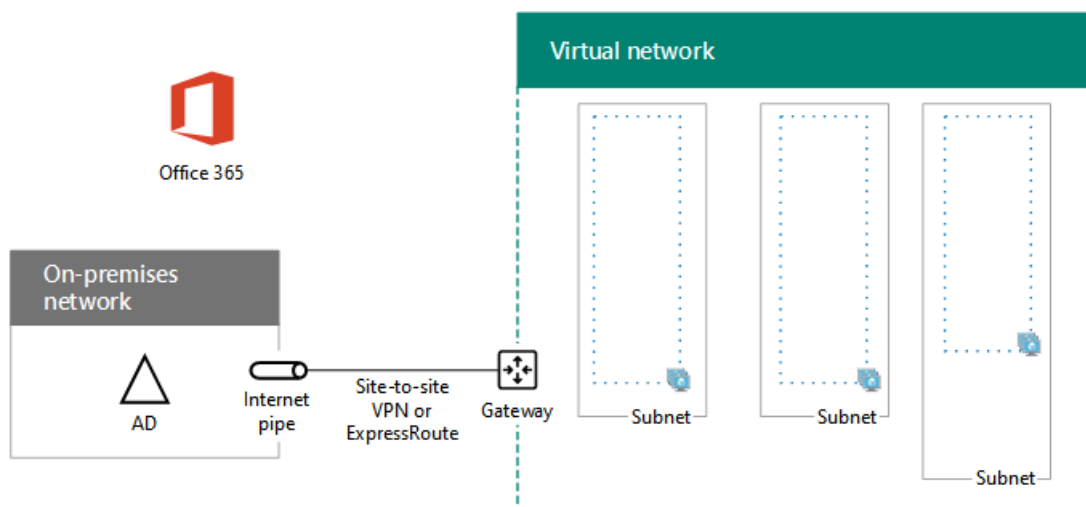
```

$locName="<the Azure location for your new resource group>"
$rgName="<Table R - Item 1 - Resource group name column>"
$avName="<Table A - Item 1 - Availability set name column>"
New-AzAvailabilitySet -ResourceGroupName $rgName -Name $avName -Location $locName -Sku Aligned -
PlatformUpdateDomainCount 5 -PlatformFaultDomainCount 2
$rgName="<Table R - Item 2 - Resource group name column>"
$avName="<Table A - Item 2 - Availability set name column>"
New-AzAvailabilitySet -ResourceGroupName $rgName -Name $avName -Location $locName -Sku Aligned -
PlatformUpdateDomainCount 5 -PlatformFaultDomainCount 2
$rgName="<Table R - Item 3 - Resource group name column>"
$avName="<Table A - Item 3 - Availability set name column>"
New-AzAvailabilitySet -ResourceGroupName $rgName -Name $avName -Location $locName -Sku Aligned -
PlatformUpdateDomainCount 5 -PlatformFaultDomainCount 2

```

This is the configuration resulting from the successful completion of this phase.

Phase 1: The Azure infrastructure for high availability federated authentication for Microsoft 365



Next step

Use [Phase 2: Configure domain controllers](#) to continue with the configuration of this workload.

See Also

[Deploy high availability federated authentication for Microsoft 365 in Azure](#)

[Federated identity for your Microsoft 365 dev/test environment](#)

[Microsoft 365 solution and architecture center](#)

[Understanding Microsoft 365 identity models](#)

High availability federated authentication Phase 2: Configure domain controllers

10/28/2022 • 9 minutes to read • [Edit Online](#)

In this phase of deploying high availability for Microsoft 365 federated authentication in Azure infrastructure services, you configure two domain controllers and the directory synchronization server in the Azure virtual network. Client web requests for authentication can then be authenticated in the Azure virtual network, rather than sending that authentication traffic across the site-to-site VPN connection to your on-premises network.

NOTE

Active Directory Federation Services (AD FS) cannot use Azure Active Directory (Azure AD) as a substitute for Active Directory Domain Services (AD DS) domain controllers.

You must complete this phase before moving on to [Phase 3: Configure AD FS servers](#). See [Deploy high availability federated authentication for Microsoft 365 in Azure](#) for all of the phases.

Create the domain controller virtual machines in Azure

First, you need to fill out the **Virtual machine name** column of Table M and modify virtual machine sizes as needed in the **Minimum size** column.

ITEM	VIRTUAL MACHINE NAME	GALLERY IMAGE	STORAGE TYPE	MINIMUM SIZE
1.	_____ (first domain controller, example DC1)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2
2.	_____ (second domain controller, example DC2)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2
3.	_____ (directory synchronization server, example DS1)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2
4.	_____ (first AD FS server, example ADFS1)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2
5.	_____ (second AD FS server, example ADFS2)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2

ITEM	VIRTUAL MACHINE NAME	GALLERY IMAGE	STORAGE TYPE	MINIMUM SIZE
6.	_____ (first web application proxy server, example WEB1)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2
7.	_____ (second web application proxy server, example WEB2)	Windows Server 2016 Datacenter	Standard_LRS	Standard_D2

Table M - Virtual machines for the high availability federated authentication for Microsoft 365 in Azure

For the complete list of virtual machine sizes, see [Sizes for virtual machines](#).

The following Azure PowerShell command block creates the virtual machines for the two domain controllers. Specify the values for the variables, removing the < and > characters. Note that this Azure PowerShell command block uses values from the following tables:

- Table M, for your virtual machines
- Table R, for your resource groups
- Table V, for your virtual network settings
- Table S, for your subnets
- Table I, for your static IP addresses
- Table A, for your availability sets

Recall that you defined Tables R, V, S, I, and A in [Phase 1: Configure Azure](#).

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell](#).

When you have supplied all the correct values, run the resulting block at the Azure PowerShell prompt or in the PowerShell Integrated Script Environment (ISE) on your local computer.

TIP

To generate ready-to-run PowerShell command blocks based on your custom settings, use this [Microsoft Excel configuration workbook](#).

```
# Set up variables common to both virtual machines
$locName="<your Azure location>"
$vnetName="<Table V - Item 1 - Value column>"
$subnetName="<Table S - Item 1 - Value column>"
$avName="<Table A - Item 1 - Availability set name column>"
$rgNameTier="<Table R - Item 1 - Resource group name column>"
$rgNameInfra="<Table R - Item 4 - Resource group name column>"

$rgName=$rgNameInfra
$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
```

```

$subnet=Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name $subnetName

$rgName=$rgNameTier
$avSet=Get-AzAvailabilitySet -Name $avName -ResourceGroupName $rgName

# Create the first domain controller
$vmName="<Table M - Item 1 - Virtual machine name column>"
$vmSize="<Table M - Item 1 - Minimum size column>"
$staticIP="<Table I - Item 1 - Value column>"
$diskStorageType="<Table M - Item 1 - Storage type column>"
$diskSize=<size of the extra disk for Active Directory Domain Services (AD DS) data in GB>

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$subnet -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
$diskConfig=New-AzDiskConfig -AccountType $diskStorageType -Location $locName -CreateOption Empty -
DiskSizeGB $diskSize
$dataDisk1=New-AzDisk -DiskName ($vmName + "-DataDisk1") -Disk $diskConfig -ResourceGroupName $rgName
$vm=Add-AzVMDataDisk -VM $vm -Name ($vmName + "-DataDisk1") -CreateOption Attach -ManagedDiskId
$dataDisk1.Id -Lun 1
$cred=Get-Credential -Message "Type the name and password of the local administrator account for the first
domain controller."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

# Create the second domain controller
$vmName="<Table M - Item 2 - Virtual machine name column>"
$vmSize="<Table M - Item 2 - Minimum size column>"
$staticIP="<Table I - Item 2 - Value column>"
$diskStorageType="<Table M - Item 2 - Storage type column>"
$diskSize=<size of the extra disk for AD DS data in GB>

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$subnet -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
$diskConfig=New-AzDiskConfig -AccountType $diskStorageType -Location $locName -CreateOption Empty -
DiskSizeGB $diskSize
$dataDisk1=New-AzDisk -DiskName ($vmName + "-DataDisk1") -Disk $diskConfig -ResourceGroupName $rgName
$vm=Add-AzVMDataDisk -VM $vm -Name ($vmName + "-DataDisk1") -CreateOption Attach -ManagedDiskId
$dataDisk1.Id -Lun 1
$cred=Get-Credential -Message "Type the name and password of the local administrator account for the second
domain controller."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

# Create the directory synchronization server
$vmName="<Table M - Item 3 - Virtual machine name column>"
$vmSize="<Table M - Item 3 - Minimum size column>"
$staticIP="<Table I - Item 3 - Value column>"
$diskStorageType="<Table M - Item 3 - Storage type column>"

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$subnet -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize

$cred=Get-Credential -Message "Type the name and password of the local administrator account for the
directory synchronization server."

```


Get-ScriptSystemConfiguration -Server \$server

```
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

NOTE

Because these virtual machines are for an intranet application, they are not assigned a public IP address or a DNS domain name label and exposed to the Internet. However, this also means that you cannot connect to them from the Azure portal. The **Connect** option is unavailable when you view the properties of the virtual machine. Use the Remote Desktop Connection accessory or another Remote Desktop tool to connect to the virtual machine using its private IP address or intranet DNS name.

Configure the first domain controller

Use the remote desktop client of your choice and create a remote desktop connection to the first domain controller virtual machine. Use its intranet DNS or computer name and the credentials of the local administrator account.

Next, add the extra data disk to the first domain controller with this command from a Windows PowerShell command prompt **on the first domain controller virtual machine**:

```
Get-Disk | Where PartitionStyle -eq "RAW" | Initialize-Disk -PartitionStyle MBR -PassThru | New-Partition -
AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS -NewFileSystemLabel "WSAD Data"
```

Next, test the first domain controller's connectivity to locations on your organization network by using the **ping** command to ping names and IP addresses of resources on your organization network.

This procedure ensures that DNS name resolution is working correctly (that the virtual machine is correctly configured with on-premises DNS servers) and that packets can be sent to and from the cross-premises virtual network. If this basic test fails, contact your IT department to troubleshoot the DNS name resolution and packet delivery issues.

Next, from the Windows PowerShell command prompt on the first domain controller, run the following commands:

```
$domname="<DNS domain name of the domain for which this computer will be a domain controller, such as
corp.contoso.com>"
$cred = Get-Credential -Message "Enter credentials of an account with permission to join a new domain
controller to the domain"
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Install-ADDSDomainController -InstallDns -DomainName $domname -DatabasePath "F:\NTDS" -SysvolPath
"F:\SYSVOL" -LogPath "F:\Logs" -Credential $cred
```

You will be prompted to supply the credentials of a domain administrator account. The computer will restart.

Configure the second domain controller

Use the remote desktop client of your choice and create a remote desktop connection to the second domain controller virtual machine. Use its intranet DNS or computer name and the credentials of the local administrator account.

Next, you need to add the extra data disk to the second domain controller with this command from a Windows PowerShell command prompt on the second domain controller virtual machine:

```
Get-Disk | Where PartitionStyle -eq "RAW" | Initialize-Disk -PartitionStyle MBR -PassThru | New-Partition -
AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS -NewFileSystemLabel "WSAD Data"
```

Next, run the following commands:

```
$domname="<DNS domain name of the domain for which this computer will be a domain controller, such as
corp.contoso.com>"
$cred = Get-Credential -Message "Enter credentials of an account with permission to join a new domain
controller to the domain"
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Install-ADDSDomainController -InstallDns -DomainName $domname -DatabasePath "F:\NTDS" -SysvolPath
"F:\SYSVOL" -LogPath "F:\Logs" -Credential $cred
```

You will be prompted to supply the credentials of a domain administrator account. The computer will restart.

Next, you need to update the DNS servers for your virtual network so that Azure assigns virtual machines the IP addresses of the two new domain controllers to use as their DNS servers. Fill in the variables and then run these commands from a Windows PowerShell command prompt on your local computer:

```
$rgName="<Table R - Item 4 - Resource group name column>"
$adrgName="<Table R - Item 1 - Resource group name column>"
$locName="<your Azure location>"
$vnetName="<Table V - Item 1 - Value column>"
$onpremDNSIP1="<Table D - Item 1 - DNS server IP address column>"
$onpremDNSIP2="<Table D - Item 2 - DNS server IP address column>"
$staticIP1="<Table I - Item 1 - Value column>"
$staticIP2="<Table I - Item 2 - Value column>"
$firstDCName="<Table M - Item 1 - Virtual machine name column>"
$secondDCName="<Table M - Item 2 - Virtual machine name column>"

$vnet=Get-AzVirtualNetwork -ResourceGroupName $rgName -Name $vnetName
$vnet.DhcpOptions.DnsServers.Add($staticIP1)
$vnet.DhcpOptions.DnsServers.Add($staticIP2)
$vnet.DhcpOptions.DnsServers.Remove($onpremDNSIP1)
$vnet.DhcpOptions.DnsServers.Remove($onpremDNSIP2)
Set-AzVirtualNetwork -VirtualNetwork $vnet
Restart-AzVM -ResourceGroupName $adrgName -Name $firstDCName
Restart-AzVM -ResourceGroupName $adrgName -Name $secondDCName
```

Note that we restart the two domain controllers so that they are not configured with the on-premises DNS servers as DNS servers. Because they are both DNS servers themselves, they were automatically configured with the on-premises DNS servers as DNS forwarders when they were promoted to domain controllers.

Next, we need to create an Active Directory replication site to ensure that servers in the Azure virtual network use the local domain controllers. Connect to either domain controller with a domain administrator account and run the following commands from an administrator-level Windows PowerShell prompt:

```
$vnet="<Table V - Item 1 - Value column>"
$vnetSpace="<Table V - Item 4 - Value column>"
New-ADReplicationSite -Name $vnet
New-ADReplicationSubnet -Name $vnetSpace -Site $vnet
```

Configure the directory synchronization server

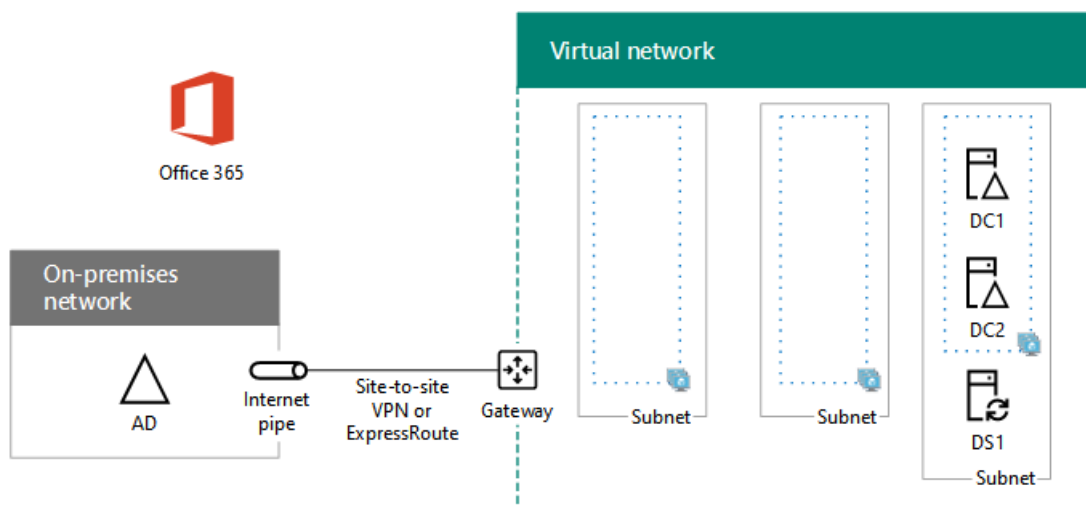
Use the remote desktop client of your choice and create a remote desktop connection to the directory synchronization server virtual machine. Use its intranet DNS or computer name and the credentials of the local administrator account.

Next, join it to the appropriate AD DS domain with these commands at the Windows PowerShell prompt.

```
$domName="<AD DS domain name to join, such as corp.contoso.com>"
$cred=Get-Credential -Message "Type the name and password of a domain account."
Add-Computer -DomainName $domName -Credential $cred
Restart-Computer
```

Here is the configuration resulting from the successful completion of this phase, with placeholder computer names.

Phase 2: The domain controllers and directory synchronization server for your high availability federated authentication infrastructure in Azure



Next step

Use [Phase 3: Configure AD FS servers](#) to continue configuring this workload.

See Also

[Deploy high availability federated authentication for Microsoft 365 in Azure](#)

[Federated identity for your Microsoft 365 dev/test environment](#)

[Microsoft 365 solution and architecture center](#)

High availability federated authentication Phase 3: Configure AD FS servers

10/28/2022 • 4 minutes to read • [Edit Online](#)

In this phase of deploying high availability for Microsoft 365 federated authentication in Azure infrastructure services, you create an internal load balancer and two AD FS servers.

You must complete this phase before moving on to [Phase 4: Configure web application proxies](#). See [Deploy high availability federated authentication for Microsoft 365 in Azure](#) for all of the phases.

Create the AD FS server virtual machines in Azure

Use the following block of PowerShell commands to create the virtual machines for the two AD FS servers. This PowerShell command set uses values from the following tables:

- Table M, for your virtual machines
- Table R, for your resource groups
- Table V, for your virtual network settings
- Table S, for your subnets
- Table I, for your static IP addresses
- Table A, for your availability sets

Recall that you defined Table M in [Phase 2: Configure domain controllers](#) and Tables R, V, S, I, and A in [Phase 1: Configure Azure](#).

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell](#).

First, you create an Azure internal load balancer for the two AD FS servers. Specify the values for the variables, removing the < and > characters. When you have supplied all the proper values, run the resulting block at the Azure PowerShell command prompt or in the PowerShell ISE.

TIP

To generate ready-to-run PowerShell command blocks based on your custom settings, use this [Microsoft Excel configuration workbook](#).

```
# Set up key variables
$locName="<your Azure location>"
$vnetName="<Table V - Item 1 - Value column>"
$subnetName="<Table R - Item 2 - Subnet name column>"
$privIP="<Table I - Item 4 - Value column>"
$rgName="<Table R - Item 4 - Resource group name column>"

$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
$subnet=Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name $subnetName

$frontendIP=New-AzLoadBalancerFrontendIpConfig -Name "ADFSServers-LBFE" -PrivateIpAddress $privIP -Subnet
$subnet
$beAddressPool=New-AzLoadBalancerBackendAddressPoolConfig -Name "ADFSServers-LBBE"

$healthProbe=New-AzLoadBalancerProbeConfig -Name WebServersProbe -Protocol "TCP" -Port 443 -
IntervalInSeconds 15 -ProbeCount 2
$lbrule=New-AzLoadBalancerRuleConfig -Name "HTTPSTraffic" -FrontendIpConfiguration $frontendIP -
BackendAddressPool $beAddressPool -Probe $healthProbe -Protocol "TCP" -FrontendPort 443 -BackendPort 443
New-AzLoadBalancer -ResourceGroupName $rgName -Name "ADFSServers" -Location $locName -LoadBalancingRule
$lbrule -BackendAddressPool $beAddressPool -Probe $healthProbe -FrontendIpConfiguration $frontendIP
```

Next, create the AD FS server virtual machines.

When you have supplied all the proper values, run the resulting block at the Azure PowerShell command prompt or in the PowerShell ISE.

```

# Set up variables common to both virtual machines
$locName="<your Azure location>"
$vnetName="<Table V - Item 1 - Value column>"
$subnetName="<Table R - Item 2 - Subnet name column>"
$avName="<Table A - Item 2 - Availability set name column>"
$rgNameTier="<Table R - Item 2 - Resource group name column>"
$rgNameInfra="<Table R - Item 4 - Resource group name column>"

$rgName=$rgNameInfra
$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
$subnet=Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name $subnetName
$backendSubnet=Get-AzVirtualNetworkSubnetConfig -Name $subnetName -VirtualNetwork $vnet
$webLB=Get-AzLoadBalancer -ResourceGroupName $rgName -Name "ADFServers"

$rgName=$rgNameTier
$avSet=Get-AzAvailabilitySet -Name $avName -ResourceGroupName $rgName

# Create the first ADFS server virtual machine
$vmName="<Table M - Item 4 - Virtual machine name column>"
$vmSize="<Table M - Item 4 - Minimum size column>"
$staticIP="<Table I - Item 5 - Value column>"
$diskStorageType="<Table M - Item 4 - Storage type column>"

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$backendSubnet -LoadBalancerBackendAddressPool $webLB.BackendAddressPools[0] -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type the name and password of the local administrator account for the first
AD FS server."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

# Create the second AD FS virtual machine
$vmName="<Table M - Item 5 - Virtual machine name column>"
$vmSize="<Table M - Item 5 - Minimum size column>"
$staticIP="<Table I - Item 6 - Value column>"
$diskStorageType="<Table M - Item 5 - Storage type column>"

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$backendSubnet -LoadBalancerBackendAddressPool $webLB.BackendAddressPools[0] -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type the name and password of the local administrator account for the second
AD FS server."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

```

NOTE

Because these virtual machines are for an intranet application, they are not assigned a public IP address or a DNS domain name label and exposed to the Internet. However, this also means that you cannot connect to them from the Azure portal. The **Connect** option is unavailable when you view the properties of the virtual machine. Use the Remote Desktop Connection accessory or another Remote Desktop tool to connect to the virtual machine using its private IP address or intranet DNS name.

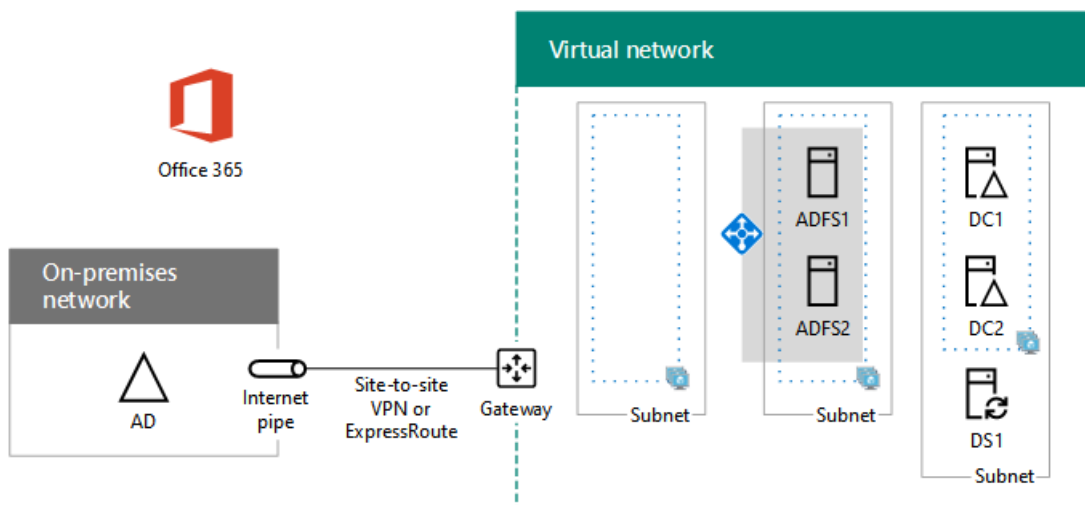
For each virtual machine, use the remote desktop client of your choice and create a remote desktop connection. Use its intranet DNS or computer name and the credentials of the local administrator account.

For each virtual machine, join them to the appropriate Active Directory Domain Services (AD DS) domain with these commands at the Windows PowerShell prompt.

```
$domName="<AD DS domain name to join, such as corp.contoso.com>"
$cred=Get-Credential -Message "Type the name and password of a domain account."
Add-Computer -DomainName $domName -Credential $cred
Restart-Computer
```

Here is the configuration resulting from the successful completion of this phase, with placeholder computer names.

Phase 3: The AD FS servers and internal load balancer for your high availability federated authentication infrastructure in Azure



Next step

Use [Phase 4: Configure web application proxies](#) to continue configuring this workload.

See Also

[Deploy high availability federated authentication for Microsoft 365 in Azure](#)

[Federated identity for your Microsoft 365 dev/test environment](#)

High availability federated authentication Phase 4: Configure web application proxies

10/28/2022 • 5 minutes to read • [Edit Online](#)

In this phase of deploying high availability for Microsoft 365 federated authentication in Azure infrastructure services, you create an internal load balancer and two AD FS servers.

You must complete this phase before moving on to [Phase 5: Configure federated authentication for Microsoft 365](#). See [Deploy high availability federated authentication for Microsoft 365 in Azure](#) for all of the phases.

Create the Internet-facing load balancer in Azure

You must create an Internet-facing load balancer so that Azure distributes the incoming client authentication traffic from the Internet evenly among the two web application proxy servers.

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell](#).

When you have supplied location and resource group values, run the resulting block at the Azure PowerShell command prompt or in the PowerShell ISE.

TIP

To generate ready-to-run PowerShell command blocks based on your custom settings, use this [Microsoft Excel configuration workbook](#).

```
# Set up key variables
$locName="<your Azure location>"
$rgName="<Table R - Item 4 - Resource group name column>"

$publicIP=New-AzPublicIpAddress -ResourceGroupName $rgName -Name "WebProxyPublicIP" -Location $locName -
AllocationMethod "Static"
$frontendIP=New-AzLoadBalancerFrontendIpConfig -Name "WebAppProxyServers-LBFE" -PublicIpAddress $publicIP
$beAddressPool=New-AzLoadBalancerBackendAddressPoolConfig -Name "WebAppProxyServers-LBBE"
$healthProbe=New-AzLoadBalancerProbeConfig -Name "WebServersProbe" -Protocol "TCP" -Port 443 -
IntervalInSeconds 15 -ProbeCount 2
$lbrule=New-AzLoadBalancerRuleConfig -Name "WebTraffic" -FrontendIpConfiguration $frontendIP -
BackendAddressPool $beAddressPool -Probe $healthProbe -Protocol "TCP" -FrontendPort 443 -BackendPort 443
New-AzLoadBalancer -ResourceGroupName $rgName -Name "WebAppProxyServers" -Location $locName -
LoadBalancingRule $lbrule -BackendAddressPool $beAddressPool -Probe $healthProbe -FrontendIpConfiguration
$frontendIP
```

To display the public IP address assigned to your Internet-facing load balancer, run these commands at the Azure PowerShell command prompt on your local computer:

```
Write-Host (Get-AzPublicIpAddress -Name "WebProxyPublicIP" -ResourceGroup $rgName).IpAddress
```

Determine your federation service FQDN and create DNS records

You need to determine the DNS name to identify your federation service name on the Internet. Azure AD Connect will configure Microsoft 365 with this name in Phase 5, which will become part of the URL that Microsoft 365 sends to connecting clients to get a security token. An example is fs.contoso.com (fs stands for federation service).

Once you have your federation service FQDN, create a public DNS domain A record for the federation service FQDN that resolves to the public IP address of the Azure Internet-facing load balancer.

NAME	TYPE	TTL	VALUE
federation service FQDN	A	3600	public IP address of the Azure Internet-facing load balancer (displayed by the Write-Host command in the previous section)

Here is an example:

NAME	TYPE	TTL	VALUE
fs.contoso.com	A	3600	131.107.249.117

Next, add a DNS address record to your organization's private DNS namespace that resolves your federation service FQDN to the private IP address assigned to the internal load balancer for the AD FS servers (Table I, item 4, Value column).

Create the web application proxy server virtual machines in Azure

Use the following block of Azure PowerShell commands to create the virtual machines for the two web application proxy servers.

Note that the following Azure PowerShell command sets use values from the following tables:

- Table M, for your virtual machines
- Table R, for your resource groups
- Table V, for your virtual network settings
- Table S, for your subnets
- Table I, for your static IP addresses
- Table A, for your availability sets

Recall that you defined Table M in [Phase 2: Configure domain controllers](#) and Tables R, V, S, I, and A in [Phase 1: Configure Azure](#).

When you have supplied all the proper values, run the resulting block at the Azure PowerShell command prompt or in the PowerShell ISE.

```

# Set up variables common to both virtual machines
$locName="<your Azure location>"
$vnetName="<Table V - Item 1 - Value column>"
$subnetName="<Table R - Item 3 - Subnet name column>"
$avName="<Table A - Item 3 - Availability set name column>"
$rgNameTier="<Table R - Item 3 - Resource group name column>"
$rgNameInfra="<Table R - Item 4 - Resource group name column>"

$rgName=$rgNameInfra
$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
$subnet=Get-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name $subnetName
$backendSubnet=Get-AzVirtualNetworkSubnetConfig -Name $subnetName -VirtualNetwork $vnet
$webLB=Get-AzLoadBalancer -ResourceGroupName $rgName -Name "WebAppProxyServers"

$rgName=$rgNameTier
$avSet=Get-AzAvailabilitySet -Name $avName -ResourceGroupName $rgName

# Create the first web application proxy server virtual machine
$vmName="<Table M - Item 6 - Virtual machine name column>"
$vmSize="<Table M - Item 6 - Minimum size column>"
$staticIP="<Table I - Item 7 - Value column>"
$diskStorageType="<Table M - Item 6 - Storage type column>"

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$backendSubnet -LoadBalancerBackendAddressPool $webLB.BackendAddressPools[0] -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type the name and password of the local administrator account for the first
web application proxy server."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

# Create the second web application proxy virtual machine
$vmName="<Table M - Item 7 - Virtual machine name column>"
$vmSize="<Table M - Item 7 - Minimum size column>"
$staticIP="<Table I - Item 8 - Value column>"
$diskStorageType="<Table M - Item 7 - Storage type column>"

$nic=New-AzNetworkInterface -Name ($vmName + "-NIC") -ResourceGroupName $rgName -Location $locName -Subnet
$backendSubnet -LoadBalancerBackendAddressPool $webLB.BackendAddressPools[0] -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type the name and password of the local administrator account for the second
web application proxy server."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name ($vmName + "-OS") -DiskSizeInGB 128 -CreateOption FromImage -
StorageAccountType $diskStorageType
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

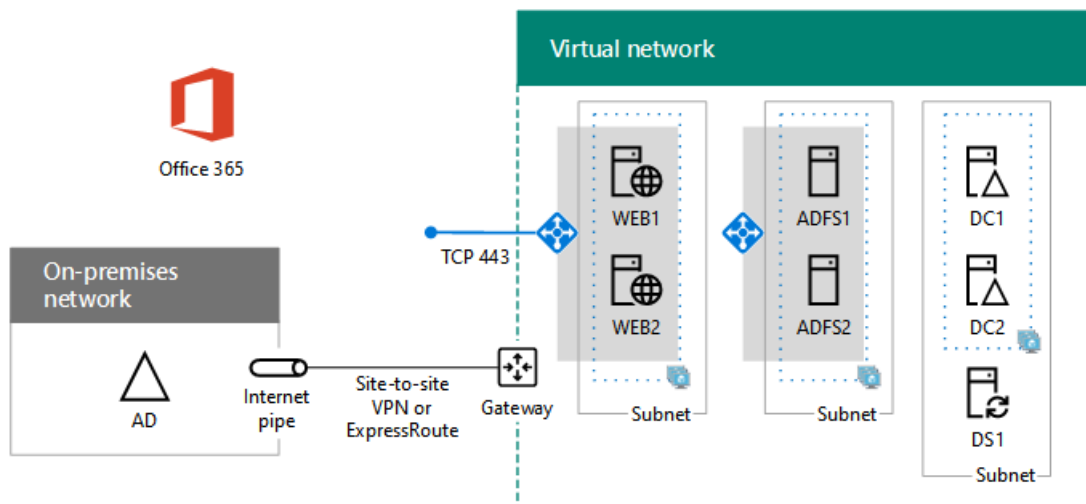
```

NOTE

Because these virtual machines are for an intranet application, they are not assigned a public IP address or a DNS domain name label and exposed to the Internet. However, this also means that you cannot connect to them from the Azure portal. The **Connect** option is unavailable when you view the properties of the virtual machine. Use the Remote Desktop Connection accessory or another Remote Desktop tool to connect to the virtual machine using its private IP address or intranet DNS name and the credentials of the local administrator account.

Here is the configuration resulting from the successful completion of this phase, with placeholder computer names.

Phase 4: The Internet-facing load balancer and web application proxy servers for your high availability federated authentication infrastructure in Azure



Next step

Use [Phase 5: Configure federated authentication for Microsoft 365](#) to continue configuring this workload.

See Also

[Deploy high availability federated authentication for Microsoft 365 in Azure](#)

[Federated identity for your Microsoft 365 dev/test environment](#)

[Microsoft 365 solution and architecture center](#)

High availability federated authentication Phase 5: Configure federated authentication for Microsoft 365

10/28/2022 • 5 minutes to read • [Edit Online](#)

In this final phase of deploying high availability federated authentication for Microsoft 365 in Azure infrastructure services, you get and install a certificate issued by a public certification authority, verify your configuration, and then install and run Azure AD Connect on the directory synchronization server. Azure AD Connect configures your Microsoft 365 subscription and your Active Directory Federation Services (AD FS) and web application proxy servers for federated authentication.

See [Deploy high availability federated authentication for Microsoft 365 in Azure](#) for all of the phases.

Get a public certificate and copy it to the directory synchronization server

Get a digital certificate from a public certification authority with the following properties:

- An X.509 certificate suitable for creating SSL connections.
- The Subject Alternative Name (SAN) extended property is set to your federation service FQDN (example: fs.contoso.com).
- The certificate must have the private key and be stored in PFX format.

Additionally, your organization computers and devices must trust the public certification authority that is issuing the digital certificate. This trust is established by having a root certificate from the public certification authority installed in the trusted root certification authorities store on your computers and devices. Computers running Microsoft Windows typically have a set of these types of certificates installed from commonly-used certification authorities. If the root certificate from your public certification authority is not already installed, you must deploy this to the computers and devices of your organization.

For more information about certificate requirements for federated authentication, see [Prerequisites for federation installation and configuration](#).

When you receive the certificate, copy it to a folder on the C: drive of the directory synchronization server. For example, name the file SSL.pfx and store it in the C:\Certs folder on the directory synchronization server.

Verify your configuration

You should now be ready to configure Azure AD Connect and federated authentication for Microsoft 365. To ensure that you are, here is a checklist:

- Your organization's public domain is added to your Microsoft 365 subscription.
- Your organization's Microsoft 365 user accounts are configured to your organization's public domain name and can successfully sign in.
- You have determined a federation service FQDN based your public domain name.
- A public DNS A record for your federation service FQDN points to the public IP address of the Internet-facing Azure load balancer for the web application proxy servers.

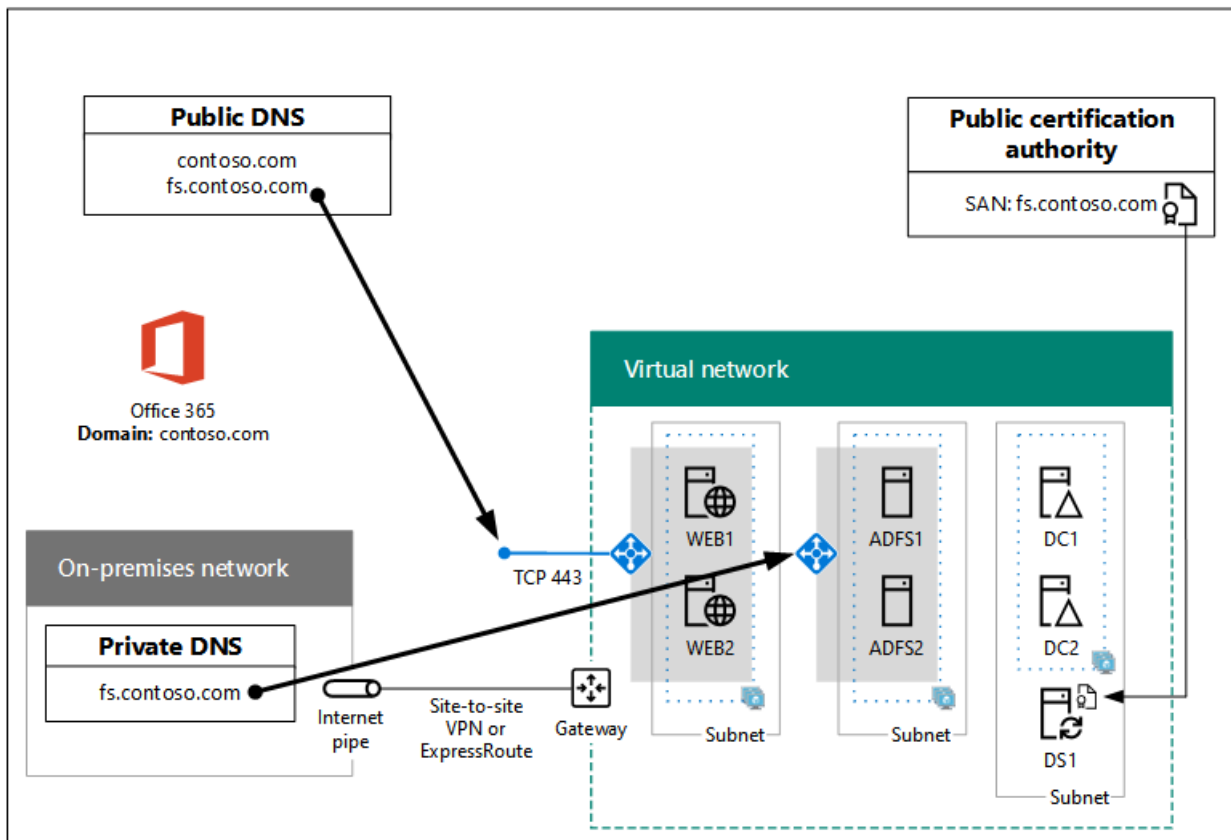
- A private DNS A record for your federation service FQDN points to the private IP address of the internal Azure load balancer for the AD FS servers.
- A public certification authority-issued digital certificate suitable for SSL connections with the SAN set to your federation service FQDN is a PFX file stored on your directory synchronization server.
- The root certificate for the public certification authority is installed in the Trusted Root Certification Authorities store on your computers and devices.

Here is an example for the Contoso organization:

An example configuration for a high availability federated authentication infrastructure in Azure

Example configuration for the Contoso Corporation

Federation service FQDN=fs.contoso.com



Run Azure AD Connect to configure federated authentication

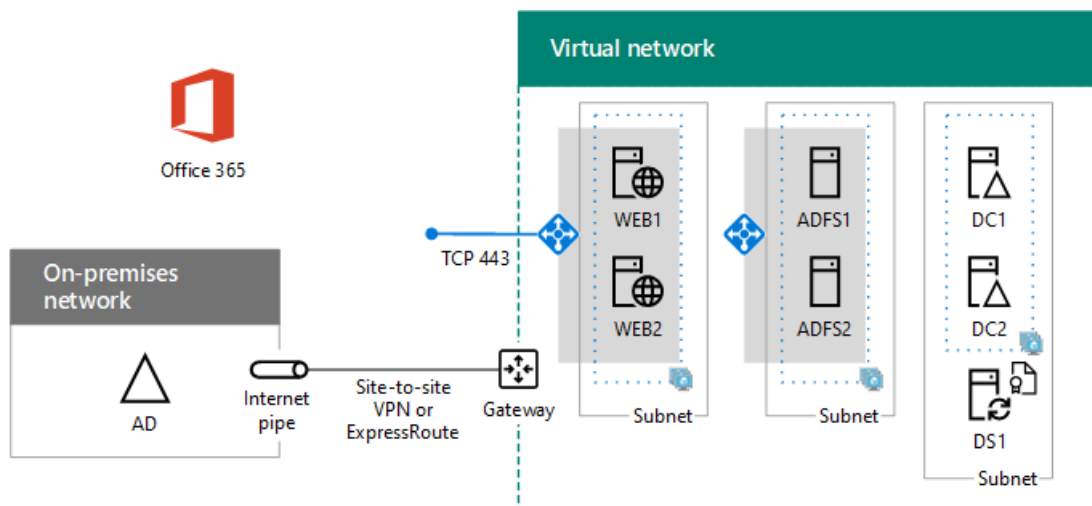
The Azure AD Connect tool configures the AD FS servers, the web application proxy servers, and Microsoft 365 for federated authentication with these steps:

1. Create a remote desktop connection to your directory synchronization server with a domain account that has local administrator privileges.
2. From the desktop of the directory synchronization server, open Internet Explorer and go to <https://aka.ms/aadconnect>.
3. On the **Microsoft Azure Active Directory Connect** page, click **Download**, and then click **Run**.
4. On the **Welcome to Azure AD Connect** page, click **I agree**, and then click **Continue**.
5. On the **Express Settings** page, click **Customize**.
6. On the **Install required components** page, click **Install**.

7. On the **User sign-in** page, click **Federation with AD FS**, and then click **Next**.
8. On the **Connect to Azure AD** page, type the name and password of a **Azure AD DC admin**, or **Global admin** account for your Microsoft 365 subscription, and then click **Next**.
9. On the **Connect your directories** page, ensure that your on-premises Active Directory Domain Services (AD DS) forest is selected in **Forest**, type the name and password of a domain administrator account, click **Add Directory**, and then click **Next**.
10. On the **Azure AD sign-in configuration** page, click **Next**.
11. On the **Domain and OU filtering** page, click **Next**.
12. On the **Uniquely identifying your users** page, click **Next**.
13. On the **Filter users and devices** page, click **Next**.
14. On the **Optional features** page, click **Next**.
15. On the **AD FS farm** page, click **Configure a new AD FS farm**.
16. Click **Browse** and specify the location and name of the SSL certificate from the public certification authority.
17. When prompted, type the certificate password, and then click **OK**.
18. Verify that the **Subject Name** and **Federation Service Name** are set to your federation service FQDN, and then click **Next**.
19. On the **AD FS servers** page, type your first AD FS server's name (Table M - Item 4 - Virtual machine name column), and then click **Add**.
20. Type your second AD FS server's name (Table M - Item 5 - Virtual machine name column), click **Add**, and then click **Next**.
21. On the **Web Application Proxy servers** page, type your first web application proxy server's name (Table M - Item 6 - Virtual machine name column), and then click **Add**.
22. Type your second web application proxy server's name (Table M - Item 7 - Virtual machine name column), click **Add**, and then click **Next**.
23. On the **Domain Administrator credentials** page, type the user name and password of a domain administrator account, and then click **Next**.
24. On the **AD FS service account** page, type the user name and password of an enterprise administrator account, and then click **Next**.
25. On the **Azure AD Domain** page, in **Domain**, select your organization's DNS domain name, and then click **Next**.
26. On the **Ready to configure** page, click **Install**.
27. On the **Installation complete** page, click **Verify**. You should see two messages indicating that both the intranet and Internet configuration was successfully verified.
 - The intranet message should list the private IP address of your Azure internal load balancer for your AD FS servers.
 - The Internet message should list the public IP address of your Azure Internet-facing load balancer for your web application proxy servers.
28. On the **Installation complete** page, click **Exit**.

Here is the final configuration, with placeholder names for the servers.

Phase 5: The final configuration of a high availability federated authentication infrastructure in Azure



Your high availability federated authentication infrastructure for Microsoft 365 in Azure is complete.

See Also

[Deploy high availability federated authentication for Microsoft 365 in Azure](#)

[Federated identity for your Microsoft 365 dev/test environment](#)

[Microsoft 365 solution and architecture center](#)

[Federated identity for Microsoft 365](#)

SharePoint Server 2013 Disaster Recovery in Microsoft Azure

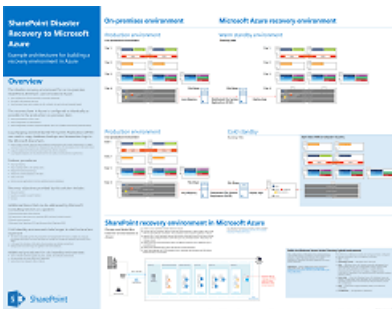
10/28/2022 • 32 minutes to read • [Edit Online](#)

Using Azure, you can create a disaster-recovery environment for your on-premises SharePoint farm. This article describes how to design and implement this solution.

Watch the SharePoint Server 2013 disaster recovery overview video

When disaster strikes your SharePoint on-premises environment, your top priority is to get the system running again quickly. Disaster recovery with SharePoint is quicker and easier when you have a backup environment already running in Microsoft Azure. This video explains the main concepts of a SharePoint warm failover environment and complements the full details available in this article.

Use this article with the following solution model: **SharePoint Disaster Recovery in Microsoft Azure**.



[PDF](#) | [Visio](#)

Use Azure Infrastructure Services for disaster recovery

Many organizations do not have a disaster recovery environment for SharePoint, which can be expensive to build and maintain on-premises. Azure Infrastructure Services provides compelling options for disaster recovery environments that are more flexible and less expensive than the on-premises alternatives.

The advantages for using Azure Infrastructure Services include:

- **Fewer costly resources** Maintain and pay for fewer resources than on-premises disaster recovery environments. The number of resources depends on which disaster-recovery environment you choose: cold standby, warm standby, or hot standby.
- **Better resource flexibility** In the event of a disaster, easily scale out your recovery SharePoint farm to meet load requirements. Scale in when you no longer need the resources.
- **Lower datacenter commitment** Use Azure Infrastructure Services instead of investing in a secondary datacenter in a different region.

There are less-complex options for organizations just getting started with disaster recovery and advanced options for organizations with high-resilience requirements. The definitions for cold, warm, and hot standby environments are a little different when the environment is hosted on a cloud platform. The following table describes these environments for building a SharePoint recovery farm in Azure.

Table: Recovery environments

TYPE OF RECOVERY ENVIRONMENT	DESCRIPTION
Hot	A fully sized farm is provisioned, updated, and running on standby.
Warm	The farm is built and virtual machines are running and updated. Recovery includes attaching content databases, provisioning service applications, and crawling content. The farm can be a smaller version of the production farm and then scaled out to serve the full user base.
Cold	The farm is fully built, but the virtual machines are stopped. Maintaining the environment includes starting the virtual machines from time to time, patching, updating, and verifying the environment. Start the full environment in the event of a disaster.

It's important to evaluate your organization's Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). These requirements determine which environment is the most appropriate investment for your organization.

The guidance in this article describes how to implement a warm standby environment. You can also adapt it to a cold standby environment, although you need to follow additional procedures to support this kind of environment. This article does not describe how to implement a hot standby environment.

For more information about disaster recovery solutions, see [High availability and disaster recovery concepts in SharePoint 2013](#) and [Choose a disaster recovery strategy for SharePoint 2013](#).

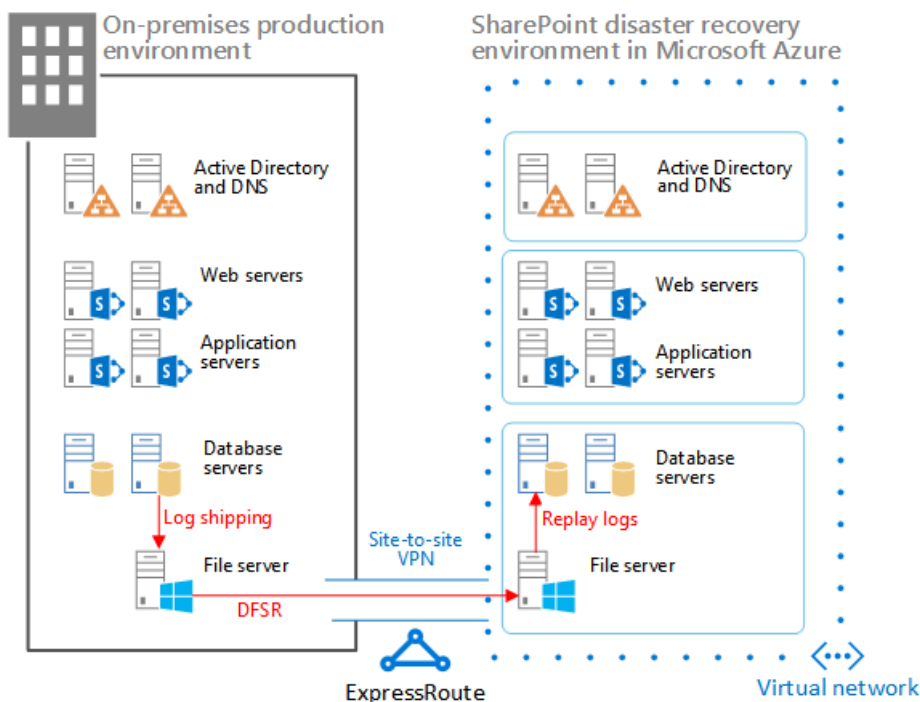
Solution description

The warm standby disaster-recovery solution requires the following environment:

- An on-premises SharePoint production farm
- A recovery SharePoint farm in Azure
- A site-to-site VPN connection between the two environments

The following figure illustrates these three elements.

Figure: Elements of a warm standby solution in Azure



SQL Server log shipping with Distributed File System Replication (DFSR) is used to copy database backups and transaction logs to the recovery farm in Azure:

- DFSR transfers logs from the production environment to the recovery environment. In a WAN scenario, DFSR is more efficient than shipping the logs directly to the secondary server in Azure.
- Logs are replayed to the SQL Server in the recovery environment in Azure.
- You don't attach log-shipped SharePoint content databases in the recovery environment until a recovery exercise is performed.

Perform the following steps to recover the farm:

1. Stop log shipping.
2. Stop accepting traffic to the primary farm.
3. Replay the final transaction logs.
4. Attach the content databases to the farm.
5. Restore service applications from the replicated services databases.
6. Update Domain Name System (DNS) records to point to the recovery farm.
7. Start a full crawl.

We recommend that you rehearse these steps regularly and document them to help ensure that your live recovery runs smoothly. Attaching content databases and restoring service applications can take some time and typically involves some manual configuration.

After a recovery is performed, this solution provides the items listed in the following table.

Table: Solution recovery objectives

ITEM	DESCRIPTION
Sites and content	Sites and content are available in the recovery environment.

ITEM	DESCRIPTION
A new instance of search	In this warm standby solution, search is not restored from search databases. Search components in the recovery farm are configured as similarly as possible to the production farm. After the sites and content are restored, a full crawl is started to rebuild the search index. You do not need to wait for the crawl to complete to make the sites and content available.
Services	Services that store data in databases are restored from the log-shipped databases. Services that do not store data in databases are simply started. Not all services with databases need to be restored. The following services do not need to be restored from databases and can simply be started after failover: Usage and Health Data Collection State service Word automation Any other service that doesn't use a database

You can work with Microsoft Consulting Services (MCS) or a partner to address more-complex recovery objectives. These are summarized in the following table.

Table: Other items that can be addressed by MCS or a partner

ITEM	DESCRIPTION
Synchronizing custom farm solutions	Ideally, the recovery farm configuration is identical to the production farm. You can work with a consultant or partner to evaluate whether custom farm solutions are replicated and whether the process is in place for keeping the two environments synchronized.
Connections to data sources on-premises	It might not be practical to replicate connections to back-end data systems, such as backup domain controller (BDC) connections and search content sources.
Search restore scenarios	Because enterprise search deployments tend to be fairly unique and complex, restoring search from databases requires a greater investment. You can work with a consultant or partner to identify and implement search restore scenarios that your organization might require.

The guidance provided in this article assumes that the on-premises farm is already designed and deployed.

Detailed architecture

Ideally, the recovery farm configuration in Azure is identical to the production farm on-premises, including the following:

- The same representation of server roles
- The same configuration of customizations
- The same configuration of search components

The environment in Azure can be a smaller version of the production farm. If you plan to scale out the recovery farm after failover, it's important that each type of server role be initially represented.

Some configurations might not be practical to replicate in the failover environment. Be sure to test the failover procedures and environment to help ensure that the failover farm provides the expected service level.

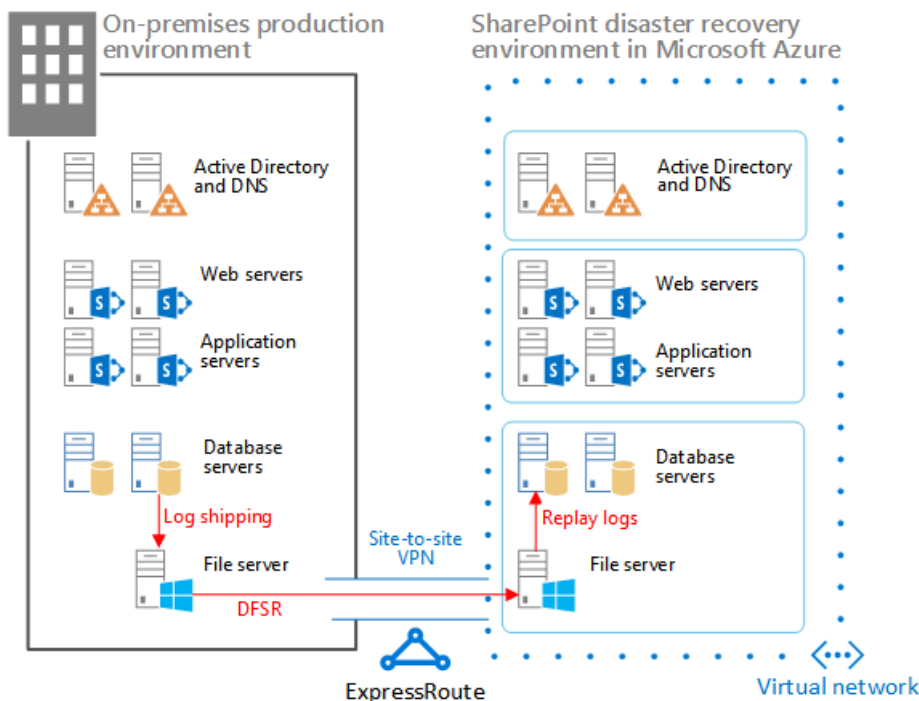
This solution doesn't prescribe a specific topology for a SharePoint farm. The focus of this solution is to use Azure for the failover farm and to implement log shipping and DFSR between the two environments.

Warm standby environments

In a warm standby environment, all virtual machines in the Azure environment are running. The environment is ready for a failover exercise or event.

The following figure illustrates a disaster recovery solution from an on-premises SharePoint farm to an Azure-based SharePoint farm that is configured as a warm standby environment.

Figure: Topology and key elements of a production farm and a warm standby recovery farm



In this diagram:

- Two environments are illustrated side by side: the on-premises SharePoint farm and the warm standby farm in Azure.
- Each environment includes a file share.
- Each farm includes four tiers. To achieve high availability, each tier includes two servers or virtual machines that are configured identically for a specific role, such as front-end services, distributed cache, back-end services, and databases. It isn't important in this illustration to call out specific components. The two farms are configured identically.
- The fourth tier is the database tier. Log shipping is used to copy logs from the secondary database server in the on-premises environment to the file share in the same environment.
- DFSR copies files from the file share in the on-premises environment to the file share in the Azure environment.
- Log shipping replays the logs from the file share in the Azure environment to the primary replica in the SQL Server AlwaysOn availability group in the recovery environment.

Cold standby environments

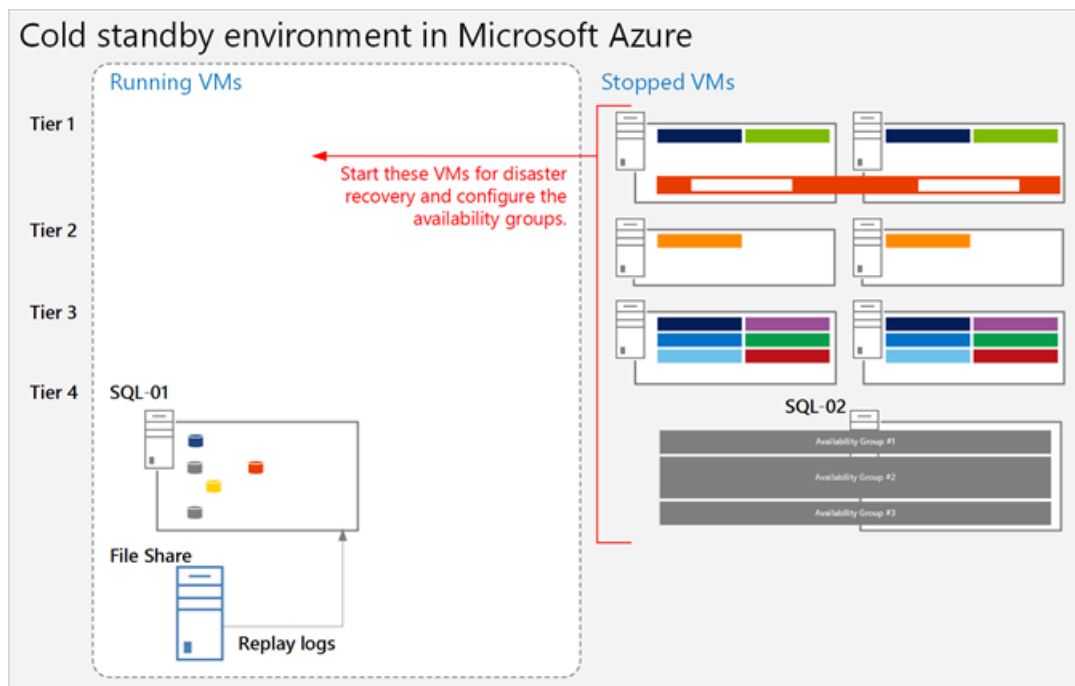
In a cold standby environment, most of the SharePoint farm virtual machines can be shut down. (We

recommend occasionally starting the virtual machines, such as every two weeks or once a month, so that each virtual machine can sync with the domain.) The following virtual machines in the Azure recovery environment must remain running to help ensure continuous operations of log shipping and DFSR:

- The file share
- The primary database server
- At least one virtual machine running Windows Server Active Directory Domain Services and DNS

The following figure shows an Azure failover environment in which the file share virtual machine and the primary SharePoint database virtual machine are running. All other SharePoint virtual machines are stopped. The virtual machine that is running Windows Server Active Directory and DNS is not shown.

Figure: Cold standby recovery farm with running virtual machines



After failover to a cold standby environment, all virtual machines are started, and the method to achieve high availability of the database servers must be configured, such as SQL Server AlwaysOn availability groups.

If multiple storage groups are implemented (databases are spread across more than one SQL Server high availability set), the primary database for each storage group must be running to accept the logs associated with its storage group.

Skills and experience

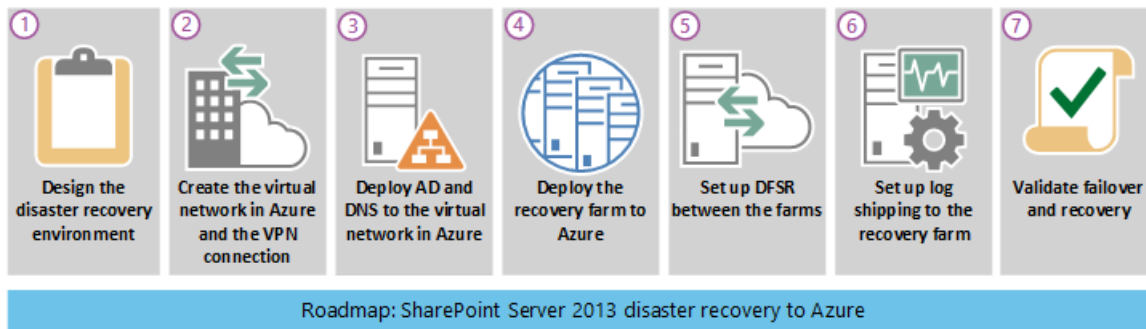
Multiple technologies are used in this disaster recovery solution. To help ensure that these technologies interact as expected, each component in the on-premises and Azure environment must be installed and configured correctly. We recommend that the person or team who sets up this solution have a strong working knowledge of and hands-on skills with the technologies described in the following articles:

- [Distributed File System \(DFS\) Replication Services](#)
- [Windows Server Failover Clustering \(WSFC\) with SQL Server](#)
- [AlwaysOn Availability Groups \(SQL Server\)](#)
- [Back Up and Restore of SQL Server Databases](#)
- [SharePoint Server 2013 installation and farm deployment](#)
- [Microsoft Azure](#)

Finally, we recommend scripting skills that you can use to automate tasks associated with these technologies. It's possible to use the available user interfaces to complete all the tasks described in this solution. However, a manual approach can be time consuming and error prone and delivers inconsistent results.

In addition to Windows PowerShell, there are also Windows PowerShell libraries for SQL Server, SharePoint Server, and Azure. Don't forget T-SQL, which can also help reduce the time to configure and maintain your disaster-recovery environment.

Disaster recovery roadmap



This roadmap assumes that you already have a SharePoint Server 2013 farm deployed in production.

Table: Roadmap for disaster recovery

PHASE	DESCRIPTION
Phase 1	Design the disaster recovery environment.
Phase 2	Create the Azure virtual network and VPN connection.
Phase 3	Deploy Windows Active Directory and Domain Name Services to the Azure virtual network.
Phase 4	Deploy the SharePoint recovery farm in Azure.
Phase 5	Set up DFSR between the farms.
Phase 6	Set up log shipping to the recovery farm.
Phase 7	Validate failover and recovery solutions. This includes the following procedures and technologies: Stop log shipping. Restore the backups. Crawl content. Recover services. Manage DNS records.

Phase 1: Design the disaster recovery environment

Use the guidance in [Microsoft Azure Architectures for SharePoint 2013](#) to design the disaster-recovery environment, including the SharePoint recovery farm. You can use the graphics in the [SharePoint Disaster Recovery Solution in Azure](#) Visio file to start the design process. We recommend that you design the entire environment before beginning any work in the Azure environment.

In addition to the guidance provided in [Microsoft Azure Architectures for SharePoint 2013](#) for designing the virtual network, VPN connection, Active Directory, and SharePoint farm, be sure to add a file share role to the

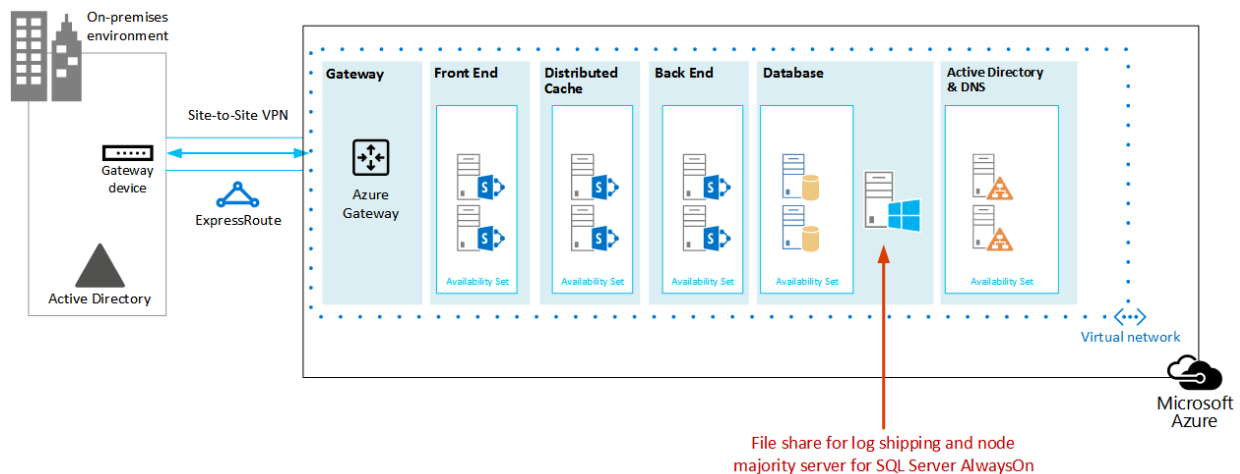
Azure environment.

To support log shipping in a disaster-recovery solution, a file share virtual machine is added to the subnet where the database roles reside. The file share also serves as the third node of a Node Majority for the SQL Server AlwaysOn availability group. This is the recommended configuration for a standard SharePoint farm that uses SQL Server AlwaysOn availability groups.

NOTE

It is important to review the prerequisites for a database to participate in a SQL Server AlwaysOn availability group. For more information, see [Prerequisites, Restrictions, and Recommendations for AlwaysOn Availability Groups](#).

Figure: Placement of a file server used for a disaster recovery solution



In this diagram, a file share virtual machine is added to the same subnet in Azure that contains the database server roles. Do not add the file share virtual machine to an availability set with other server roles, such as the SQL Server roles.

If you are concerned about the high availability of the logs, consider taking a different approach by using [SQL Server backup and restore with Azure Blob Storage Service](#). This is a new feature in Azure that saves logs directly to a blob storage URL. This solution does not include guidance about using this feature.

When you design the recovery farm, keep in mind that a successful disaster recovery environment accurately reflects the production farm that you want to recover. The size of the recovery farm is not the most important thing in the recovery farm's design, deployment, and testing. Farm scale varies from organization to organization based on business requirements. It might be possible to use a scaled-down farm for a short outage or until performance and capacity demands require you to scale the farm.

Configure the recovery farm as identically as possible to the production farm so that it meets your service level agreement (SLA) requirements and provides the functionality that you need to support your business. When you design the disaster recovery environment, also look at your change management process for your production environment. We recommend that you extend the change management process to the recovery environment by updating the recovery environment at the same interval as the production environment. As part of the change management process, we recommend maintaining a detailed inventory of your farm configuration, applications, and users.

Phase 2: Create the Azure virtual network and VPN connection

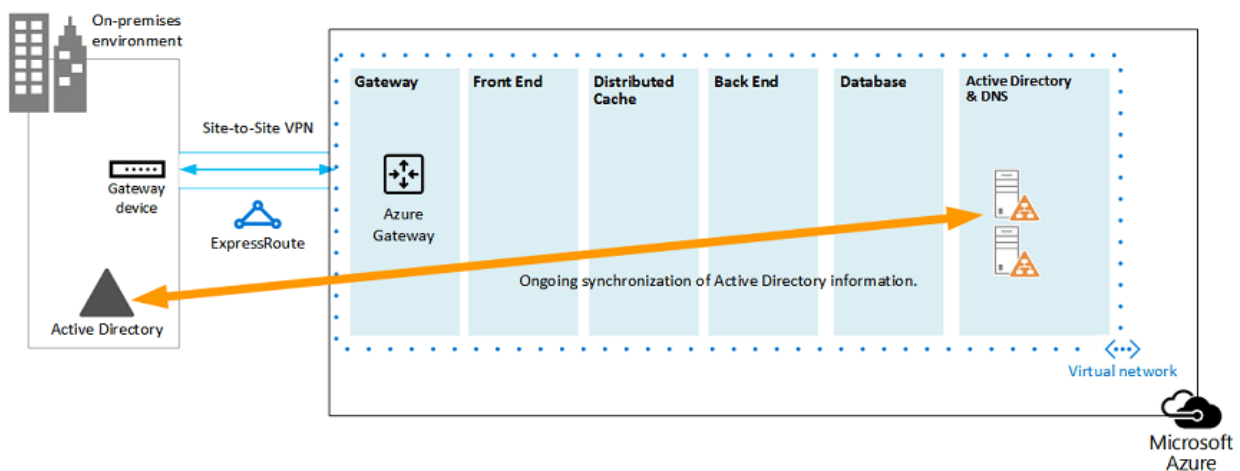
[Connect an on-premises network to a Microsoft Azure virtual network](#) shows you how to plan and deploy the virtual network in Azure and how to create the VPN connection. Follow the guidance in the topic to complete the following procedures:

- Plan the private IP address space of the Virtual Network.
- Plan the routing infrastructure changes for the Virtual Network.
- Plan firewall rules for traffic to and from the on-premises VPN device.
- Create the cross-premises virtual network in Azure.
- Configure routing between your on-premises network and the Virtual Network.

Phase 3: Deploy Active Directory and Domain Name Services to the Azure virtual network

This phase includes deploying both Windows Server Active Directory and DNS to the Virtual Network in a hybrid scenario as described in [Microsoft Azure Architectures for SharePoint 2013](#) and as illustrated in the following figure.

Figure: Hybrid Active Directory domain configuration



In the illustration, two virtual machines are deployed to the same subnet. These virtual machines are each hosting two roles: Active Directory and DNS.

Before deploying Active Directory in Azure, read [Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines](#). These guidelines help you determine whether you need a different architecture or different configuration settings for your solution.

For detailed guidance on setting up a domain controller in Azure, see [Install a Replica Active Directory Domain Controller in Azure Virtual Networks](#).

Before this phase, you didn't deploy virtual machines to the Virtual Network. The virtual machines for hosting Active Directory and DNS are likely not the largest virtual machines you need for the solution. Before you deploy these virtual machines, first create the largest virtual machine that you plan to use in your Virtual Network. This helps ensure that your solution lands on a tag in Azure that allows the largest size you need. You do not need to configure this virtual machine at this time. Simply create it, and set it aside. If you do not do this, you might run into a limitation when you try to create larger virtual machines later, which was an issue at the time this article was written.

Phase 4: Deploy the SharePoint recovery farm in Azure

Deploy the SharePoint farm in your Virtual Network according to your design plans. It might be helpful to review [Planning for SharePoint 2013 on Azure Infrastructure Services](#) before you deploy SharePoint roles in Azure.

Consider the following practices that we learned by building our proof of concept environment:

- Create virtual machines by using the Azure portal or PowerShell.
- Azure and Hyper-V do not support dynamic memory. Be sure this is factored into your performance and capacity plans.
- Restart virtual machines through the Azure interface, not from the virtual machine logon itself. Using the Azure interface works better and is more predictable.
- If you want to shut down a virtual machine to save costs, use the Azure interface. If you shut down from the virtual machine logon, charges continue to accrue.
- Use a naming convention for the virtual machines.
- Pay attention to which datacenter location the virtual machines are being deployed.
- The automatic scaling feature in Azure is not supported for SharePoint roles.
- Do not configure items in the farm that will be restored, such as site collections.

Phase 5: Set up DFSR between the farms

To set up file replication by using DFSR, use the DNS Management snap-in. However, before the DFSR setup, log on to your on-premises file server and Azure file server and enable the service in Windows.

From the Server Manager Dashboard, complete the following steps:

- Configure the local server.
- Start the **Add Roles and Features Wizard**.
- Open the **File and Storage Services** node.
- Select **DFS Namespaces** and **DFS replication**.
- Click **Next** to finish the wizard steps.

The following table provides links to DFSR reference articles and blog posts.

Table: Reference articles for DFSR

TITLE	DESCRIPTION
Replication	DFS Management TechNet topic with links for replication
DFS Replication: Survival Guide	Wiki with links to DFS information
DFS Replication: Frequently Asked Questions	DFS Replication TechNet topic
Jose Barreto's Blog	Blog written by a Principal Program Manager on the File Server team at Microsoft
The Storage Team at Microsoft - File Cabinet Blog	Blog about file services and storage features in Windows Server

Phase 6: Set up log shipping to the recovery farm

Log shipping is the critical component for setting up disaster recovery in this environment. You can use log shipping to automatically send transaction log files for databases from a primary database server instance to a secondary database server instance. To set up log shipping, see [Configure log shipping in SharePoint 2013](#).

IMPORTANT

Log shipping support in SharePoint Server is limited to certain databases. For more information, see [Supported high availability and disaster recovery options for SharePoint databases \(SharePoint 2013\)](#).

Phase 7: Validate failover and recovery

The goal of this final phase is to verify that the disaster recovery solution works as planned. To do this, create a failover event that shuts down the production farm and starts up the recovery farm as a replacement. You can start a failover scenario manually or by using scripts.

The first step is to stop incoming user requests for farm services or content. You can do this by disabling DNS entries or by shutting down the front-end web servers. After the farm is "down," you can fail over to the recovery farm.

Stop log shipping

You must stop log shipping before farm recovery. Stop log shipping on the secondary server in Azure first, and then stop it on the primary server on-premises. Use the following script to stop log shipping on the secondary server first and then on the primary server. The database names in the script might be different, depending on your environment.

```
-- This script removes log shipping from the server.
-- Commands must be executed on the secondary server first and then on the primary server.

SET NOCOUNT ON
DECLARE @PriDB nvarchar(max)
,@SecDB nvarchar(250)
,@PriSrv nvarchar(250)
,@SecSrv nvarchar(250)

Set @PriDB= ''
SET @PriDB = UPPER(@PriDB)
SET @PriDB = REPLACE(@PriDB, ' ', '')
SET @PriDB = '''' + REPLACE(@PriDB, ',', ''', ''') + ''''

Set @SecDB = @PriDB

Exec ( 'Select ''exec master..sp_delete_log_shipping_secondary_database '' + '''''''' +
prm.primary_database + ''''''''
from msdb.dbo.log_shipping_monitor_primary prm INNER JOIN msdb.dbo.log_shipping_primary_secondaries sec ON
prm.primary_database=sec.secondary_database
where prm.primary_database in ( ' + @PriDB + ' )')

Exec ( 'Select ''exec master..sp_delete_log_shipping_primary_secondary '' + '''''''' + prm.Primary_Database
+ ''''''', '''''' + sec.Secondary_Server + ''''''', '''''' + sec.Secondary_database + ''''''''
from msdb.dbo.log_shipping_monitor_primary prm INNER JOIN msdb.dbo.log_shipping_primary_secondaries sec ON
prm.primary_database=sec.secondary_database
where prm.primary_database in ( ' + @PriDB + ' )')

Exec ( 'Select ''exec master..sp_delete_log_shipping_primary_database '' + '''''''' + prm.primary_database
+ ''''''''
from msdb.dbo.log_shipping_monitor_primary prm INNER JOIN msdb.dbo.log_shipping_primary_secondaries sec ON
prm.primary_database=sec.secondary_database
where prm.primary_database in ( ' + @PriDB + ' )')

Exec ( 'Select ''exec master..sp_delete_log_shipping_secondary_primary '' + '''''''' + prm.primary_server +
''''''', '''''' + prm.primary_database + ''''''''
from msdb.dbo.log_shipping_monitor_primary prm INNER JOIN msdb.dbo.log_shipping_primary_secondaries sec ON
prm.primary_database=sec.secondary_database
where prm.primary_database in ( ' + @PriDB + ' )')
```

Restore the backups

Backups must be restored in the order in which they were created. Before you can restore a particular transaction log backup, you must first restore the following previous backups without rolling back uncommitted transactions (that is, by using `WITH NORECOVERY`):

- The full database backup and the last differential backup - Restore these backups, if any exist, taken before the particular transaction log backup. Before the most recent full or differential database backup was created, the database was using the full recovery model or bulk-logged recovery model.
- All transaction log backups - Restore any transaction log backups taken after the full database backup or the differential backup (if you restore one) and before the particular transaction log backup. Log backups must be applied in the sequence in which they were created, without any gaps in the log chain.

To recover the content database on the secondary server so that the sites render, remove all database connections before recovery. To restore the database, run the following SQL statement.

```
restore database WSS_Content with recovery
```

IMPORTANT

When you use T-SQL explicitly, specify either **WITH NORECOVERY** or **WITH RECOVERY** in every RESTORE statement to eliminate ambiguity—this is very important when writing scripts. After the full and differential backups are restored, the transaction logs can be restored in SQL Server Management Studio. Also, because log shipping is already stopped, the content database is in a standby state, so you must change the state to full access.

In SQL Server Management Studio, right-click the **WSS_Content** database, point to **Tasks > Restore**, and then click **Transaction Log** (if you have not restored the full backup, this is not available). For more information, see [Restore a Transaction Log Backup \(SQL Server\)](#).

Crawl the content source

You must start a full crawl for each content source to restore the Search Service. Note that you lose some analytics information from the on-premises farm, such as search recommendations. Before you start the full crawls, use the Windows PowerShell cmdlet **Restore-SPEnterpriseSearchServiceApplication** and specify the log-shipped and replicated Search Administration database, **Search_Service__DB_<GUID>**. This cmdlet gives the search configuration, schema, managed properties, rules, and sources and creates a default set of the other components.

To start a full crawl, complete the following steps:

1. In the SharePoint 2013 Central Administration, go to **Application Management > Service Applications > Manage service applications**, and then click the Search Service application that you want to crawl.
2. On the **Search Administration** page, click **Content Sources**, point to the content source that you want, click the arrow, and then click **Start Full Crawl**.

Recover farm services

The following table shows how to recover services that have log-shipped databases, the services that have databases but are not recommended to restore with log shipping, and the services that do not have databases.

IMPORTANT

Restoring an on-premises SharePoint database into the Azure environment will not recover any SharePoint services that you did not already install in Azure manually.

Table: Service application database reference

RESTORE THESE SERVICES FROM LOG-SHIPPED DATABASES	THESE SERVICES HAVE DATABASES, BUT WE RECOMMEND THAT YOU START THESE SERVICES WITHOUT RESTORING THEIR DATABASES	THESE SERVICES DO NOT STORE DATA IN DATABASES; START THESE SERVICES AFTER FAILOVER
Machine Translation Service Managed Metadata Service Secure Store Service User Profile. (Only the Profile and Social Tagging databases are supported. The Synchronization database is not supported.) Microsoft SharePoint Foundation Subscription Settings Service	Usage and Health Data Collection State service Word automation	Excel Services PerformancePoint Services PowerPoint Conversion Visio Graphics Service Work Management

The following example shows how to restore the Managed Metadata service from a database.

This uses the existing Managed_Metadata_DB database. This database is log shipped, but there is no active service application on the secondary farm, so it needs to be connected after the service application is in place.

First, use `New-SPMetadataServiceApplication`, and specify the `DatabaseName` switch with the name of the restored database.

Next, configure the new Managed Metadata Service Application on the secondary server, as follows:

- Name: Managed Metadata Service
- Database server: The database name from the shipped transaction log
- Database name: Managed_Metadata_DB
- Application pool: SharePoint Service Applications

Manage DNS records

You must manually create DNS records to point to your SharePoint farm.

In most cases where you have multiple front-end web servers, it makes sense to take advantage of the Network Load Balancing feature in Windows Server 2012 or a hardware load balancer to distribute requests among the web-front-end servers in your farm. Network load balancing can also help reduce risk by distributing requests to the other servers if one of your web-front-end servers fails.

Typically, when you set up network load balancing, your cluster is assigned a single IP address. You then create a DNS host record in the DNS provider for your network that points to the cluster. (For this project, we put a DNS server in Azure for resiliency in case of an on-premises datacenter failure.) For instance, you can create a DNS record, in DNS Manager in Active Directory, for example, called `https://sharepoint.contoso.com`, that points to the IP address for your load-balanced cluster.

For external access to your SharePoint farm, you can create a host record on an external DNS server with the same URL that clients use on your intranet (for example, `https://sharepoint.contoso.com`) that points to an external IP address in your firewall. (A best practice, using this example, is to set up split DNS so that the internal DNS server is authoritative for `contoso.com` and routes requests directly to the SharePoint farm cluster, rather than routing DNS requests to your external DNS server.) You can then map the external IP address to the internal IP address of your on-premises cluster so that clients find the resources they are looking for.

From here, you might run into a couple of different disaster-recovery scenarios:

Example scenario: The on-premises SharePoint farm is unavailable because of hardware failure in the on-premises SharePoint farm. In this case, after you have completed the steps for failover to the Azure

SharePoint farm, you can configure network load balancing on the recovery SharePoint farm's web-front-end servers, the same way you did with the on-premises farm. You can then redirect the host record in your internal DNS provider to point to the recovery farm's cluster IP address. Note that it can take some time before cached DNS records on clients are refreshed and point to the recovery farm.

Example scenario: The on-premises datacenter is lost completely. This scenario might occur due to a natural disaster, such as a fire or flood. In this case, for an enterprise, you would likely have a secondary datacenter hosted in another region as well as your Azure subnet that has its own directory services and DNS. As in the previous disaster scenario, you can redirect your internal and external DNS records to point to the Azure SharePoint farm. Again, take note that DNS-record propagation can take some time.

If you are using host-named site collections, as recommended in [Host-named site collection architecture and deployment \(SharePoint 2013\)](#), you might have several site collections hosted by the same web application in your SharePoint farm, with unique DNS names (for example, `https://sales.contoso.com` and `https://marketing.contoso.com`). In this case, you can create DNS records for each site collection that point to your cluster IP address. After a request reaches your SharePoint web-front-end servers, they handle routing each request to the appropriate site collection.

Microsoft proof-of-concept environment

We designed and tested a proof-of-concept environment for this solution. The design goal for our test environment was to deploy and recover a SharePoint farm that we might find in a customer environment. We made several assumptions, but we knew that the farm needed to provide all of the out-of-the-box functionality without any customizations. The topology was designed for high availability by using best practice guidance from the field and product group.

The following table describes the Hyper-V virtual machines that we created and configured for the on-premises test environment.

Table: Virtual machines for on-premises test

SERVER NAME	ROLE	CONFIGURATION
DC1	Domain controller with Active Directory.	Two processors From 512 MB through 4 GB of RAM 1 x 127-GB hard disk
RRAS	Server configured with the Routing and Remote Access Service (RRAS) role.	Two processors 2-8 GB of RAM 1 x 127-GB hard disk
FS1	File server with shares for backups and an end point for DFSR.	Four processors 2-12 GB of RAM 1 x 127-GB hard disk 1 x 1-TB hard disk (SAN) 1 x 750-GB hard disk
SP-WFE1, SP-WFE2	Front-end web servers.	Four processors 16 GB of RAM
SP-APP1, SP-APP2, SP-APP3	Application servers.	Four processors 2-16 GB of RAM

SERVER NAME	ROLE	CONFIGURATION
SP-SQL-HA1, SP-SQL-HA2	Database servers, configured with SQL Server 2012 AlwaysOn availability groups to provide high availability. This configuration uses SP-SQL-HA1 and SP-SQL-HA2 as the primary and secondary replicas.	Four processors 2-16 GB of RAM

The following table describes drive configurations for the Hyper-V virtual machines that we created and configured for the front-end web and application servers for the on-premises test environment.

Table: Virtual machine drive requirements for the Front End Web and Application servers for the on-premises test

DRIVE LETTER	SIZE	DIRECTORY NAME	PATH
C	80	System drive	<DriveLetter>:\Program Files\Microsoft SQL Server\
E	80	Log drive (40 GB)	<DriveLetter>:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA
F	80	Page (36 GB)	<DriveLetter>:\Program Files\Microsoft SQL Server\MSSQL\DATA

The following table describes drive configurations for the Hyper-V virtual machines created and configured to serve as the on-premises database servers. On the **Database Engine Configuration** page, access the **Data Directories** tab to set and confirm the settings shown in the following table.

Table: Virtual machine drive requirements for the database server for the on-premises test

DRIVE LETTER	SIZE	DIRECTORY NAME	PATH
C	80	Data root directory	<DriveLetter>:\Program Files\Microsoft SQL Server\
E	500	User database directory	<DriveLetter>:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA
F	500	User database log directory	<DriveLetter>:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA
G	500	Temp DB directory	<DriveLetter>:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA

DRIVE LETTER	SIZE	DIRECTORY NAME	PATH
H	500	Temp DB log directory	<DriveLetter>:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA

Setting up the test environment

During the different deployment phases, the test team typically worked on the on-premises architecture first and then on the corresponding Azure environment. This reflects the general real-world cases where in-house production farms are already running. What is even more important is that you should know the current production workload, capacity, and typical performance. In addition to building a disaster recovery model that can meet business requirements, you should size the recovery farm servers to deliver a minimum level of service. In a cold or warm standby environment, a recovery farm is typically smaller than a production farm. After the recovery farm is stable and in production, the farm can be scaled up and out to meet workload requirements.

We deployed our test environment in the following three phases:

- Set up the hybrid infrastructure
- Provision the servers
- Deploy the SharePoint farms

Set up the hybrid infrastructure

This phase involved setting up a domain environment for the on-premises farm and for the recovery farm in Azure. In addition to the normal tasks associated with configuring Active Directory, the test team implemented a routing solution and a VPN connection between the two environments.

Provision the servers

In addition to the farm servers, it was necessary to provision servers for the domain controllers and configure a server to handle RRAS as well as the site-to-site VPN. Two file servers were provisioned for the DFSR service, and several client computers were provisioned for testers.

Deploy the SharePoint farms

The SharePoint farms were deployed in two stages in order to simplify environment stabilization and troubleshooting, if required. During the first stage, each farm was deployed on the minimum number of servers for each tier of the topology to support the required functionality.

We created the database servers with SQL Server installed before creating the SharePoint 2013 servers. Because this was a new deployment, we created the availability groups before deploying SharePoint. We created three groups based on MCS best practice guidance.

NOTE

Create placeholder databases so that you can create availability groups before the SharePoint installation. For more information, see [Configure SQL Server 2012 AlwaysOn Availability Groups for SharePoint 2013](#)

We created the farm and joined additional servers in the following order:

- Provision SP-SQL-HA1 and SP-SQL-HA2.
- Configure AlwaysOn and create the three availability groups for the farm.
- Provision SP-APP1 to host Central Administration.
- Provision SP-WFE1 and SP-WFE2 to host the distributed cache.

We used the *skipRegisterAsDistributedCachehost* parameter when we ran **psconfig.exe** at the command line. For more information, see [Plan for feeds and the Distributed Cache service in SharePoint Server 2013](#).

We repeated the following steps in the recovery environment:

- Provision AZ-SQL-HA1 and AZ-SQL-HA2.
- Configure AlwaysOn and create the three availability groups for the farm.
- Provision AZ-APP1 to host Central Administration.
- Provision AZ-WFE1 and AZ-WFE2 to host the distributed cache.

After we configured the distributed cache and added test users and test content, we started stage two of the deployment. This required scaling out the tiers and configuring the farm servers to support the high-availability topology described in the farm architecture.

The following table describes the virtual machines, subnets, and availability sets we set up for our recovery farm.

Table: Recovery farm infrastructure

SERVER NAME	ROLE	CONFIGURATION	SUBNET	AVAILABILITY SET
spDRAD	Domain controller with Active Directory	Two processors From 512 MB through 4 GB of RAM 1 x 127-GB hard disk	sp-ADservers	
AZ-SP-FS	File server with shares for backups and an endpoint for DFSR	A5 configuration: Two processors 14 GB of RAM 1 x 127-GB hard disk 1 x 135-GB hard disk 1 x 127-GB hard disk 1 x 150-GB hard disk	sp-databaseservers	DATA_SET
AZ-WFE1, AZ -WFE2	Front End Web servers	A5 configuration: Two processors 14 GB of RAM 1 x 127-GB hard disk	sp-webservers	WFE_SET
AZ -APP1, AZ -APP2, AZ -APP3	Application servers	A5 configuration: Two processors 14 GB of RAM 1 x 127-GB hard disk	sp-applicationservers	APP_SET
AZ -SQL-HA1, AZ -SQL-HA2	Database servers and primary and secondary replicas for AlwaysOn availability groups	A5 configuration: Two processors 14 GB of RAM	sp-databaseservers	DATA_SET

Operations

After the test team stabilized the farm environments and completed functional testing, they started the following operations tasks required to configure the on-premises recovery environment:

- Configure full and differential backups.

- Configure DFSR on the file servers that transfer transaction logs between the on-premises environment and the Azure environment.
- Configure log shipping on the primary database server.
- Stabilize, validate, and troubleshoot log shipping, as required. This included identifying and documenting any behavior that might cause issues, such as network latency, which would cause log shipping or DFSR file synchronization failures.

Databases

Our failover tests involved the following databases:

- WSS_Content
- ManagedMetadata
- Profile DB
- Sync DB
- Social DB
- Content Type Hub (a database for a dedicated Content Type Syndication Hub)

Troubleshooting tips

The section explains the problems we encountered during our testing and their solutions.

Using the Term Store Management Tool caused the error, "The Managed Metadata Store or Connection is currently not available."

Ensure that the application pool account used by the web application has the Read Access to Term Store permission.

Custom term sets are not available in the site collection

Check for a missing service application association between your content site collection and your content type hub. In addition, under the **Managed Metadata - <site collection name> Connection** properties screen, make sure this option is enabled: **This service application is the default storage location for column specific term sets.**

The Get-ADForest Windows PowerShell command generates the error, "The term 'Get-ADForest' is not recognized as the name of a cmdlet, function, script file, or operable program."

When setting up user profiles, you need the Active Directory forest name. In the Add Roles and Features Wizard, ensure that you have enabled the Active Directory Module for Windows PowerShell (under the **Remote Server Administration Tools>Role Administration Tools>AD DS and AD LDS Tools** section). In addition, run the following commands before using **Get-ADForest** to help ensure that your software dependencies are loaded.

```
Import-Module ServerManager
Import-Module ActiveDirectory
```

Availability group creation fails at Starting the 'AlwaysOn_health' XEvent session on '<server name>'

Ensure that both nodes of your failover cluster are in the Status "Up" and not "Paused" or "Stopped".

SQL Server log shipping job fails with access denied error trying to connect to the file share

Ensure that your SQL Server Agent is running under network credentials, instead of the default credentials.

SQL Server log shipping job indicates success, but no files are copied

This happens because the default backup preference for an availability group is **Prefer Secondary**. Ensure that you run the log shipping job from the secondary server for the availability group instead of the primary; otherwise, the job will fail silently.

Managed Metadata service (or other SharePoint service) fails to start automatically after installation

Services might take several minutes to start, depending on the performance and current load of your SharePoint Server. Manually click **Start** for the service and provide adequate time for startup while occasionally refreshing the Services on Server screen to monitor its status. In case the service remains stopped, enable SharePoint diagnostic logging, attempt to start the service again, and then check the log for errors. For more information, see [Configure diagnostic logging in SharePoint 2013](#)

After changing DNS to the Azure failover environment, client browsers continue to use the old IP address for the SharePoint site

Your DNS change might not be visible to all clients immediately. On a test client, perform the following command from an elevated command prompt and attempt to access the site again.

```
Ipconfig /flushdns
```

Additional resources

[Supported high availability and disaster recovery options for SharePoint databases](#)

[Configure SQL Server 2012 AlwaysOn Availability Groups for SharePoint 2013](#)

See Also

[Microsoft 365 solution and architecture center](#)

Manage Microsoft 365 user accounts

10/28/2022 • 3 minutes to read • [Edit Online](#)

You can manage Microsoft 365 user accounts in several different ways, depending on your configuration. You can manage user accounts in the [Microsoft 365 admin center](#), [PowerShell](#), in Active Directory Domain Services (AD DS), or in the Azure Active Directory (Azure AD) admin portal.

As soon as you purchase Microsoft 365, the [Microsoft 365 admin center](#) and PowerShell can be used to manage accounts. When managing cloud identities, every person in your organization has a separate user account name and password. If you want to integrate with your on-premises infrastructure and have user accounts synchronized with Microsoft 365, you can use Azure AD Connect to provide synchronization of identities and passwords for single sign-on (SSO) functionality.

Plan for where and how you will manage your user accounts

Where and how you can manage your user accounts depends on the identity model you want to use for your Microsoft 365. The two overall models are cloud-only and hybrid.

Cloud-only

You create and manage users in the [Microsoft 365 admin center](#). You can also use PowerShell or the Azure AD admin center.

Hybrid

User accounts are synchronized with Microsoft 365 from AD DS, so you must use on-premises AD DS tools to manage user accounts.

Managing Accounts

When deciding which way your organization will create and manage accounts, consider the following requirements:

- The directory synchronization software needs to be installed on servers within your on-premises environment to connect the identities between Microsoft 365 and your AD DS.
- Any directory synchronization option, including SSO options, requires that your AD DS attributes meet standards. The specifics of what attributes are used in your directory and what cleanup (if any) is needed are described in [Prepare for directory synchronization to Microsoft 365](#).
- Plan how you are going to create Microsoft 365 accounts.

The following table lists the different account management tools.

TOOL	NOTES
Microsoft 365 admin center	Add users individually or in bulk Provides a simple web interface to add and change user accounts. Can't be used to change users if directory synchronization is enabled (location and license assignment can be set). Can't be used with SSO options.

TOOL	NOTES
Windows PowerShell	Manage Microsoft 365 with Windows PowerShell Allows you to add users in bulk users by using a Windows PowerShell script. Can be used to assign location and licenses to accounts, regardless of how the accounts are created.
Bulk import	Add several users at the same time Allows you to import a CSV file to add a group of users to Microsoft 365. Can't be used with SSO options.
Azure AD	You get a free edition of Azure AD with your Microsoft 365 subscription. You can perform functions like self-service password reset for cloud users, and customization of the Sign-in and Access Panel pages by using the free edition. To get enhanced functionality, you can upgrade to the basic edition, Azure AD Premium P1, or Azure AD Premium P2. See Azure AD editions for the list of supported features.
Directory synchronization	Integrating your on-premises identities with Azure AD For directory synchronization with or without password synchronization, use Azure AD Connect with express settings . For multiple forests and SSO options, use Custom Installation of Azure AD Connect . Provides the infrastructure that's necessary to enable SSO. Required for many hybrid scenarios such as staged migration and hybrid Exchange Synchronizes security and mail-enabled groups from your AD DS.

- Regardless of how you intend to add the user accounts to Microsoft 365, you need to manage several account features, such as assigning licenses, specifying location, and so on. These features can be managed long-term from the [Microsoft 365 admin center](#) or you can also [create user accounts with PowerShell](#).

If you choose to add and manage all your users through the admin center, you will specify the location and assign licenses at the same time as creating the Microsoft 365 account. As a result, not much planning is required.

IMPORTANT

Creating accounts in Microsoft 365 without assigning a license (to SharePoint Online, for example) means that the account owner can view the Microsoft 365 center but can't access any of the services within your company's subscription. After you assign a location and the license, the account is replicated to the service or services that you assigned. The user can sign in to their account and use the services that you assigned to them.

See also

[Microsoft 365 admin center](#)

[PowerShell](#)

Add several users at the same time to Microsoft 365

- Admin Help

10/28/2022 • 5 minutes to read • [Edit Online](#)

Each person on your team needs a user account before they can sign in and access Microsoft 365 services, such as email and Office. If you have a lot of people, you can add their accounts all at once from an Excel spreadsheet or other file saved in CSV format. [Not sure what CSV format is?](#)

NOTE

If you're not using the new Microsoft 365 admin center, you can turn it on by selecting the **Try the new admin center** toggle located at the top of the Home page.

Add multiple users in the Microsoft 365 admin center

1. Sign in to Microsoft 365 with your work or school account.
2. In the admin center, choose **Users** > [Active users](#).
3. Select **Add multiple users**.
4. On the **Import multiple users** panel, you can optionally download a sample CSV file with or without sample data filled in.

Your spreadsheet needs to include the **exact same column headings** as the sample one (User Name, First Name, and so on). If you use the template, open it in a text editing tool, like Notepad, and consider leaving all the data in row 1 alone, and only entering data in rows 2 and below.

Your spreadsheet also needs to include values for the user name (like bob@contoso.com) and a display name (like Bob Kelly) for each user.

```
User Name,First Name,Last Name,Display Name,Job Title,Department,Office Number,Office Phone,Mobile Phone,Fax,Address,City,State or Province,ZIP or Postal Code,Country or Region
chris@contoso.com,Chris,Green,Chris Green,IT Manager,Information Technology,123451,123-555-1211,123-555-6641,123-555-6700,1 Microsoft way,Redmond,Wa,98052,United States
ben@contoso.com,Ben,Andrews,Ben Andrews,IT Manager,Information Technology,123452,123-555-1212,123-555-6642,123-555-6700,1 Microsoft way,Redmond,Wa,98052,United States
david@contoso.com,David,Longmuir,David Longmuir,IT Manager,Information Technology,123453,123-555-1213,123-555-6643,123-555-6700,1 Microsoft way,Redmond,Wa,98052,United States
cynthia@contoso.com,Cynthia,Carey,Cynthia Carey,IT Manager,Information Technology,123454,123-555-1214,123-555-6644,123-555-6700,1 Microsoft way,Redmond,Wa,98052,United States
melissa@contoso.com,Melissa,MacBeth,Melissa MacBeth,IT Manager,Information Technology,123455,123-555-1215,123-555-6645,123-555-6700,1 Microsoft way,Redmond,Wa,98052,United States
```

5. Enter a file path into the box, or choose **Browse** to browse to the CSV file location, then choose **Verify**.

If there are problems with the file, the problem is displayed in the panel. You can also download a log file.

6. On the **Set user options** dialog you can set the sign-in status and choose the product license that will be assigned to all users.
7. On the **View your result** dialog you can choose to send the results to either yourself or other users

(passwords will be in plain text) and you can see how many users were created, and if you need to purchase more licenses to assign to some of the new users.

Next steps

- Now that these people have accounts, they need to [Download and install or reinstall Microsoft 365 or Office 2016 on a PC or Mac](#). Each person on your team can install Microsoft 365 on up to 5 PCs or Macs.
- Each person can also [Set up Office apps and email on a mobile device](#) on up to 5 tablets and 5 phones, such as iPhones, iPads, and Android phones and tablets. This way they can edit Office files from anywhere.

See [Set up Microsoft 365 for business](#) for an end-to-end list of the setup steps.

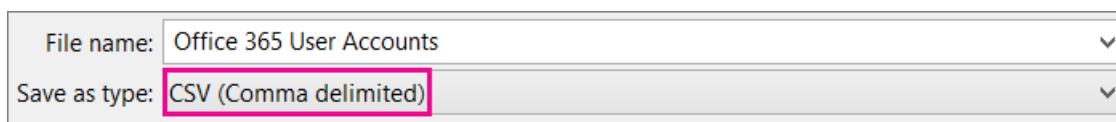
More information about how to add users to Microsoft 365

Not sure what CSV format is?

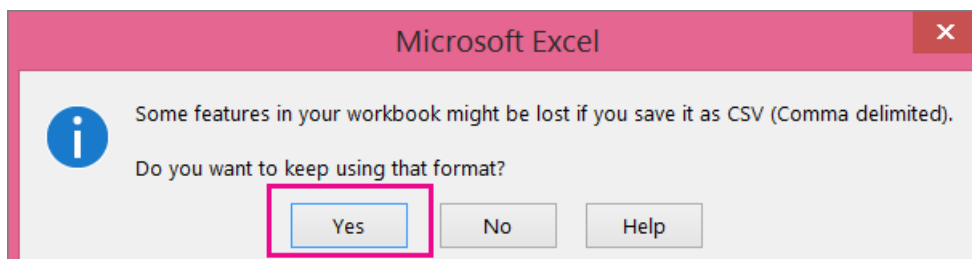
A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

You can download [this sample spreadsheet](#) as a starting point. Remember that Microsoft 365 requires column headings in the first row so don't replace them with something else.

Save the file with a new name, and specify CSV format.



When you save the file, you'll probably get a prompt that some features in your workbook will be lost if you save the file in CSV format. This is okay. Click **Yes** to continue.



Tips for formatting your spreadsheet

- **Do I need the same column headings as in the sample spreadsheet?** Yes. The sample spreadsheet contains column headings in the first row. These headings are required. For each user you want to add to Microsoft 365, create a row under the heading. If you add, change, or delete any of the column headings, Microsoft 365 might not be able to create users from the information in the file.
- **What if I don't have all the information required for each user?** The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.
- **How small or large can the spreadsheet be?** The spreadsheet must have at least two rows. One is for the column headings (the user data column label) and one for the user. You cannot have more than 251 rows. If you need to import more than 250 users, you can create more than one spreadsheet.
- **What languages can I use?** When you create your spreadsheet, you can enter user data column labels in any language or characters, but you must not change the order of the labels, as shown in the sample.

You can then make entries into the fields, using any language or characters, and save your file in a Unicode or UTF-8 format.

- **What if I'm adding users from different countries or regions?** Create a separate spreadsheet for each area. You'll need to step through the Bulk add users wizard which each spreadsheet, giving a single location of all users included in the file that you're working with.
- **Is there a limit to the number of characters I can use?** The following table shows the user data column labels and the maximum character length for each in the sample spreadsheet.

USER DATA COLUMN LABEL	MAXIMUM CHARACTER LENGTH
User Name (Required)	79 including the at sign (@), in the format name@domain.<extension>. The user's alias cannot exceed 50 characters, and the domain name cannot exceed 48 characters.
First Name	64
Last Name	64
Display Name (required)	256
Job Title	64
Department	64
Office Number	128
Office Phone	64
Mobile Phone	64
Fax	64
Address	1023
City	128
State or Province	128
ZIP or Postal Code	40
Country or Region	128

Still having problems when adding users to Microsoft 365?

- **Double-check that the spreadsheet is formatted correctly.** Check the column headings to make sure they match the headings in the sample file. Make sure you're following the rules for character lengths and that each field is separated by a comma.
- **If you don't see the new users in Microsoft 365 right away, wait a few minutes.** It can take a little while for changes to go across all the services in Microsoft 365.

Related articles

Add users individually or in bulk to Microsoft 365

Assign Microsoft 365 licenses to user accounts

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

For the cloud-only identity model, you can assign Microsoft 365 licenses to user accounts as they are created, depending on how you create them.

For the hybrid identity model, when Active Directory Domain Services (AD DS) user accounts are synchronized for the first time, they are not automatically assigned a location or a Microsoft 365 license. **You must configure each user account with a user location prior to or along with assigning a license.**

In either case, you must assign a license to user accounts so your users can access Microsoft 365 services, such as email and Microsoft Teams.

You can assign licenses to user accounts either individually or automatically through group membership.

To assign Microsoft 365 licenses to individual user accounts, you can use:

- [The Microsoft 365 admin center](#)
- [PowerShell](#)
- The Azure AD admin center

Group-based licensing

You can configure security groups in Azure AD to automatically assign licenses from a set of subscriptions to all the members of the group. This is known as *group-based licensing*. If a user account is added to or removed from the group, the licenses for the group's subscriptions will be automatically assigned or unassigned from the user account.

Make sure you have enough licenses for all the group members. If you run out of licenses, new users won't be assigned licenses until licenses become available.

NOTE

You should not configure group-based licensing for groups that contain Azure business to business (B2B) accounts.

For more information, see [group-based licensing in Azure AD](#).

Next steps

With the appropriate set of user accounts that have been assigned licenses, you are now ready to:

- [Implement security](#)
- [Deploy client software, such as Microsoft 365 Apps](#)
- [Set up device management](#)
- [Configure services and applications](#)

Manage Microsoft 365 user account passwords

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can manage Microsoft 365 user account passwords in several different ways, depending on your identity configuration. You can manage user accounts in the [Microsoft 365 admin center](#), in Active Directory Domain Services (AD DS), or in the Azure Active Directory (Azure AD) admin center.

Plan for where and how you will manage your user account passwords

Where and how you can manage your user accounts depends on the identity model you want to use for your Microsoft 365. The two models are cloud-only and hybrid.

Cloud-only

You manage user account passwords in:

- [The Microsoft 365 admin center](#)
- The Azure AD admin center

Hybrid

With hybrid identity, passwords are stored in AD DS so you must use on-premises AD DS tools to manage user account passwords. Even when using Password Hash Synchronization (PHS), in which Azure AD stores a hashed version of the already hashed version in AD DS, you and users must manage their passwords in AD DS.

With [password writeback](#), your users can change their AD DS passwords through Azure AD.

Prevent bad passwords

All your users should be using [Microsoft's password guidance](#) to create their user account passwords.

To prevent users from creating an easily-determined password, use Azure AD password protection, which uses both a global banned password list and an optional custom banned password list that you specify. For example, you can specify terms that are specific to your organization, such as:

- Brand names
- Product names
- Locations (for example, such as company headquarters)
- Company-specific internal terms
- Abbreviations that have specific company meaning

You can ban bad passwords [in the cloud](#) and for your [on-premises AD DS](#).

Simplify user sign-in

Azure AD Seamless Single Sign-On (Azure AD Seamless SSO) works with PHS and Pass-Through Authentication (PTA), to allow your users to sign in to services that use Azure AD user accounts without having to type in their passwords, and in many cases, their usernames. This gives your users easier access to cloud-based applications, such as Office 365, without needing any additional on-premises components such as identity federation servers.

You configure Azure AD Seamless SSO with the Azure AD Connect tool. See the [instructions to configure Azure](#)

Simplify password updates to AD DS

With password writeback, you can allow users to reset their passwords through Azure AD, which is then replicated to AD DS. Users don't need to access their on-premises AD DS to update their passwords. This is valuable to roaming or remote users who do not have a remote access connection to the on-premises network.

Password writeback is required to fully utilize Azure AD Identity Protection capabilities, such as requiring users to change their on-premises passwords when there has been a high risk of account compromise detected.

For additional information and configuration instructions, see [Azure AD SSPR with password writeback](#).

NOTE

Upgrade to the latest version of Azure AD Connect to ensure the best possible experience and new features as they are released. For more information, see [Custom installation of Azure AD Connect](#).

Simplify password resets

Self-service password reset (SSPR) allows users to reset or unlock their passwords or accounts. To alert you to misuse or abuse, you can use the detailed reporting that tracks when users access the system, along with notifications. You must enable [password writeback](#) before you can deploy password resets.

See the [instructions to roll out password reset](#).

Manage Microsoft 365 groups

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can manage Microsoft 365 groups in several different ways, depending on your configuration. You can manage user accounts in the [Microsoft 365 admin center](#), PowerShell, in Active Directory Domain Services (AD DS), or in the [Azure Active Directory \(Azure AD\) admin center](#).

Plan for where and how you will manage your groups

Where and how you can manage your user accounts depends on the identity model you want to use for your Microsoft 365. The two overall models are cloud-only and hybrid.

Cloud-only

You create and manage groups with:

- [The Microsoft 365 admin center](#)
- [PowerShell](#)
- [Azure AD admin center](#)

Hybrid

AD DS groups are synchronized with Microsoft 365 from AD DS, so you must use on-premises AD DS tools to manage these groups.

You can also create and manage Azure AD groups that are separate from AD DS groups but can contain users and groups from AD DS. In this case, you can use:

- [The Microsoft 365 admin center](#)
- [PowerShell](#)
- [Azure AD admin center](#)

Allow users to create and manage their own groups

Azure AD allows groups that can be managed by group owners instead of IT administrators. Known as *self-service group management*, this feature allows group owners who are not assigned an administrative role to create and manage security groups.

Users can request membership in a security group and that request goes to the group owner, rather than an IT administrator. This allows the day-to-day control of group membership to be delegated to team, project, or business owners who understand the business use for the group and can manage its membership.

NOTE

Self-service group management is available only for Azure AD security and Microsoft 365 groups. It is not available for mail-enabled groups, distribution lists, or any group that has been synchronized from AD DS.

For more information, see the [instructions to configure an Azure AD group for self-service management](#).

Set up dynamic group membership

Azure AD supports configuring a series of rules that automatically add or remove user accounts as members of an Azure AD group. This is known as *dynamic group membership*. The rules are based on user account attributes, such as Department or Country.

Here's how the rules are applied:

- If a new user account matches all the rules for the group, it becomes a member.
- If a user account isn't a member of the group, but its attributes change so that it matches all the rules for the group, it becomes a member of that group.
- If a user account doesn't match all the rules for the group, it isn't added to the group.
- If a user account is a member of the group, but its attributes change so that it no longer matches all the rules for the group, it is removed as a member of the group.

To use dynamic membership, you must first determine the sets of groups that have a common set of user account attributes. For example, all members of the Sales department should be in the Sales Azure AD group, based on the user account attribute Department set to "Sales".

See the [instructions to create and configure the rules for a dynamic Azure AD group](#).

Set up automatic licensing

You can configure security groups in Azure AD to automatically assign licenses from a set of subscriptions to all the members of the group. This is known as *group-based licensing*. If a user account is added to or removed from the group, the licenses for the group's subscriptions will be automatically assigned or unassigned from the user account.

For Microsoft 365 Enterprise, you'll configure Azure AD security groups to assign the appropriate Microsoft 365 Enterprise license.

Make sure you have enough licenses for all the group members. If you run out of licenses, new users won't be assigned licenses until licenses become available.

NOTE

You should not configure group-based licensing for groups that contain Azure business to business (B2B) accounts.

For more information, see [Group-based licensing basics in Azure AD](#).

See the [instructions to configure group-based licensing for an Azure security group](#).

Manage Microsoft 365 identity governance

10/28/2022 • 2 minutes to read • [Edit Online](#)

Identity governance is all about protecting, monitoring, and auditing access to critical assets while ensuring employee productivity. For example, with identity governance, you can ensure that the right users have the right access to the right resources and determine if that access changes over time.

For more information, See this [overview of identity governance for Azure Active Directory \(Azure AD\)](#).

Set up Azure AD access reviews

Azure AD access reviews allow you to review a user's access to ensure only the right people have continued access. For example:

- As a new employee joins your organization, you need to ensure they have the right access to be productive.
- As that employee moves to other teams, locations, or departments, you need to ensure that their access to previous teams, locations, or departments are removed as needed.
- When that employee or a guest leaves your organization, you need to ensure their access is removed.

This is especially important if your organization is subject to security audits to determine if user accounts have too much access, which could result in fines if in violation of industry or regional regulations.

For more information, see the [overview of access reviews](#).

See these articles to configure different types of access reviews:

- [Groups and apps](#)
- [Azure AD roles](#)
- [Azure resource roles](#)

Set up Azure AD entitlement management

With Azure AD entitlement management, you can manage the identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration.

Your employees need access to various groups, applications, and sites to perform their job. Managing this access can be challenging because requirements change, new applications are added, or users need additional access rights. When you collaborate with other organizations, you may not know who in the other organization needs access to your organization's resources, and outside users won't know what applications, groups, or sites your organization is using.

Azure AD entitlement management can help you more efficiently manage access to groups, applications, and SharePoint sites for internal and outside users.

For more information, see the [overview of Azure AD entitlement management](#).

View directory synchronization status in Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

If you have integrated your on-premises Active Directory Domain Services (AD DS) with Azure Active Directory (Azure AD) by synchronizing your on-premises environment with Microsoft 365, you can also check the status of your synchronization.

View directory synchronization status

- Sign in to the [Microsoft 365 admin center](#) and choose **DirSync Status** on the home page.
- Alternately, you can go to **Users > Active users**, and on the **Active users** page, select the **Ellipse > Directory synchronization**. On the **Directory Synchronization** pane, choose **Go to DirSync management**.

Information on the Manage directory synchronization page

The following table lists the features you can get information about on the page.

If there is a problem with your directory synchronization, the errors are listed on this page as well. For more information about different errors you might encounter, see [Identify directory synchronization errors in Microsoft 365](#).

ITEM	WHAT IT'S FOR
Domains verified	Number of domains in your Microsoft 365 tenant that you have verified you own.
Domains not verified	Domains you have added, but not verified.
Directory sync enabled	True or False. Specifies whether you have enabled directory sync.
Latest directory sync	Last time directory sync ran. Will display a warning and a link to a troubleshooting tool if the last sync was more than three days ago.
Password sync enabled	True or False. Specifies whether you have password hash sync between our on-premises and your Microsoft 365 tenant.
Last Password Sync	Last time password hash sync ran. Will display a warning and a link to a troubleshooting tool if the last sync was more than three days ago.
Directory sync client version	Contains a download link if a new version of Azure AD Connect has been released.
Directory sync service account	Displays the name of your Microsoft 365 directory sync service account.

ITEM	WHAT IT'S FOR

Monitor synchronization health

In this section, you'll install an Azure AD Connect Health agent on each of your on-premises AD DS domain controllers to monitor your identity infrastructure and the synchronization services provided by Azure AD Connect. The monitoring information is made available in an Azure AD Connect Health portal, where you can view alerts, performance monitoring, usage analytics, and other information.

The key design decision of how to use Azure AD Connect Health is based on how you are using Azure AD Connect:

- If you're using the **managed authentication** option, start with [Using Azure AD Connect Health with sync](#) to understand and configure Azure AD Connect Health.
- If you're synchronizing just the names of the accounts and groups using **federated authentication** with Active Directory Federation Services (AD FS), start with [Using Azure AD Connect Health with AD FS](#) to understand and configure Azure AD Connect Health.

When complete, you'll have:

- The Azure AD Connect Health agent installed on your on-premises identity provider servers.
- The Azure AD Connect Health portal displaying the current state of your on-premises infrastructure and synchronization activities with the Azure AD tenant for your Microsoft 365 subscription.

View directory synchronization errors in Microsoft 365

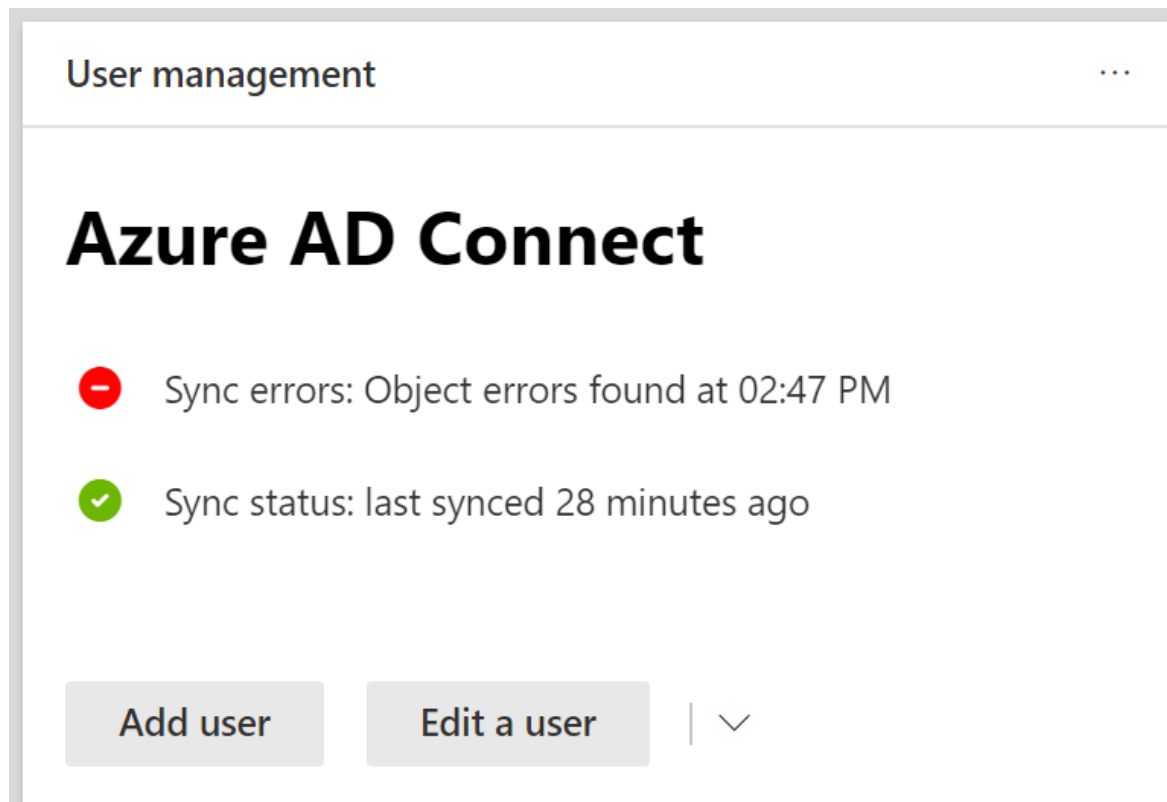
10/28/2022 • 2 minutes to read • [Edit Online](#)

You can view directory synchronization errors in the [Microsoft 365 admin center](#). Only the User object errors are displayed. To view errors with PowerShell, see [Identify objects with DirSyncProvisioningErrors](#).

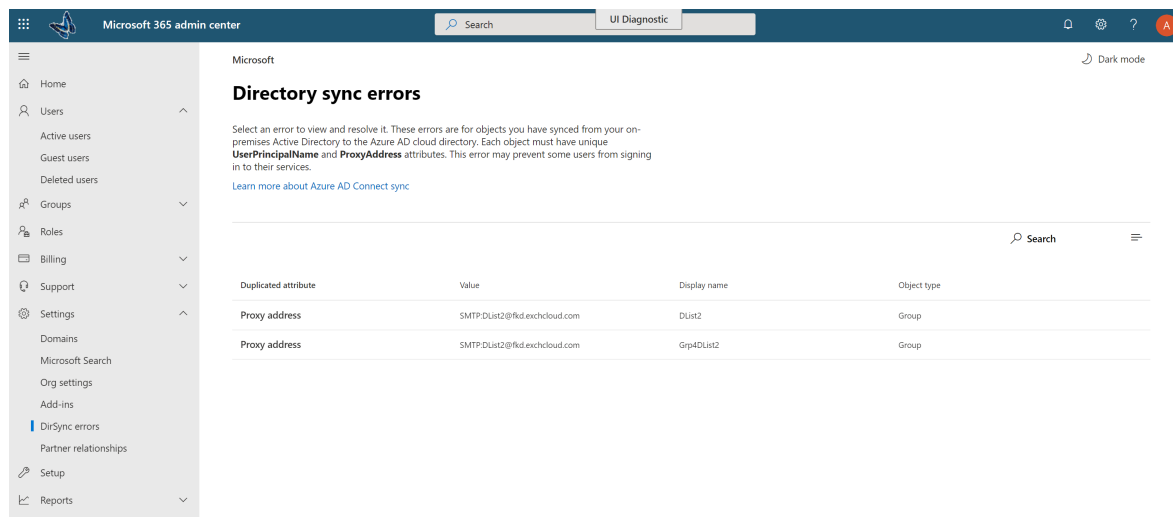
View directory synchronization errors in the Microsoft 365 admin center

To view any errors in the Microsoft 365 admin center:

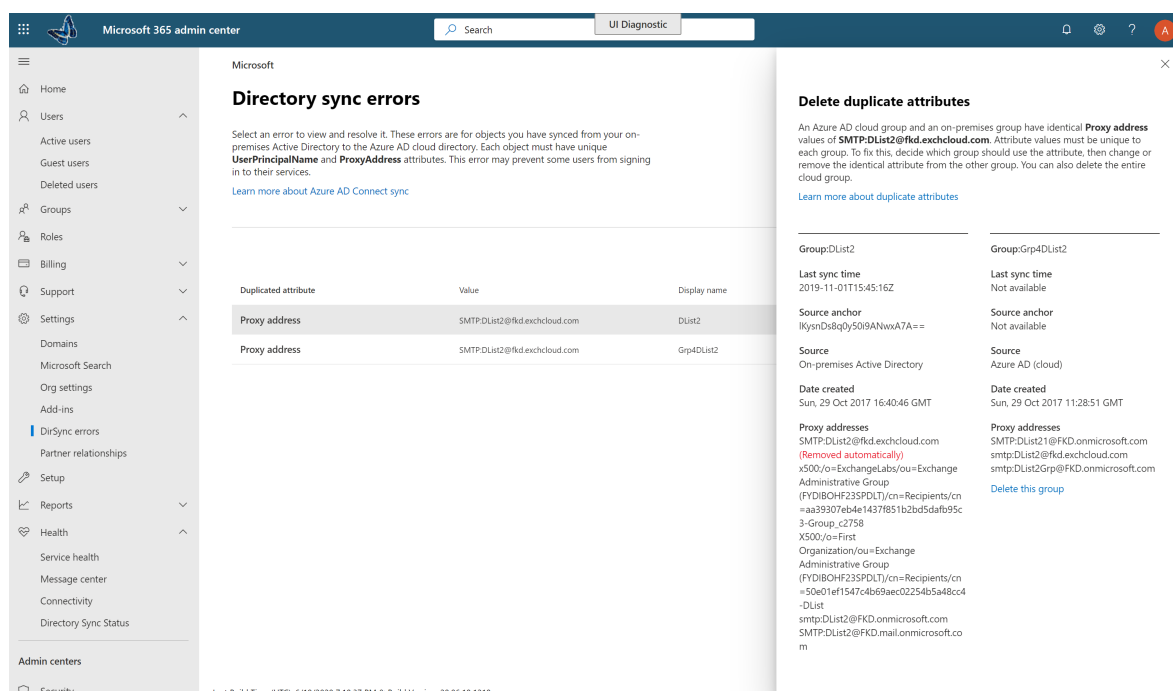
1. Sign in to the [Microsoft 365 admin center](#) with a global administrator account.
2. On the **Home** page, you'll see the **User management** card.



3. On the card, choose **Sync errors** under **Azure AD Connect** to see the errors on the **Directory sync errors** page.



4. Choose any of the errors to display the details pane with information about the error and tips on how to fix it.



After viewing, see [fixing problems with directory synchronization for Microsoft 365](#) to correct any identified issues.

Fixing problems with directory synchronization for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

With directory synchronization, you can continue to manage users and groups on-premises and synchronize additions, deletions, and changes to the cloud. But setup is a little complicated and it can sometimes be difficult to identify the source of problems. We have resources to help you identify potential issues and fix them.

How do I know if something is wrong?

The first indication that something is wrong is when the DirSync Status tile in the Microsoft 365 admin center indicates there is a problem.

You will also receive a mail (to the alternate email and to your admin email) from Microsoft 365 that indicates your tenant has encountered directory synchronization errors. For details see [Identify directory synchronization errors in Microsoft 365](#).

How do I get Azure Active Directory Connect tool?

In the [Microsoft 365 admin center](#), navigate to **Users > Active users**. Click the **More** menu (three dots) and select **Directory synchronization**.

Follow the [instructions in the wizard](#) to download Azure AD Connect.

If you are still using Azure Active Directory (Azure AD) Sync (DirSync), take a look at [How to troubleshoot Azure Active Directory Sync Tool installation and Configuration Wizard error messages in Microsoft 365](#) for information about the system requirements to install dirsnc, the permissions you need, and how to troubleshoot common errors.

To update from Azure AD Sync to Azure AD Connect, see [the upgrade instructions](#).

Resolving common causes of problems with directory synchronization in Microsoft 365

Synchronized objects aren't appearing or updating online, or I'm getting synchronization error reports from the Service.

- [Identity synchronization and duplicate attribute resiliency](#)

I have an alert in the admin center, or am receiving automated emails that there hasn't been a recent synchronization event

- [Troubleshoot connectivity issues with Azure AD Connect](#)
- [Azure AD Connect Accounts and permissions](#)
- [Azure AD Connect sync: How to manage the Azure AD service account](#)
- [Directory synchronization to Azure Active Directory stops or you're warned that sync hasn't registered in more than a day](#)

Password hashes aren't synchronizing, or I'm seeing an alert in the admin center that there hasn't been a recent password hash synchronization

- [Implementing password hash synchronization with Azure AD Connect sync](#)

I'm seeing an alert that Object quota exceeded

- We have a built-in object quota to help protect the service. If you have too many objects in your directory that need to sync to Microsoft 365, you'll have to [Contact support for business products](#) to increase your quota.

I need to know which attributes are synchronized

- You can find a list of all the attributes that are synced between on-premises and the cloud [right here](#).

I can't manage or remove objects that were synchronized to the cloud

- Are you ready to manage objects in the cloud only? Or is there an object that was deleted on-premises, but is stuck in the cloud? Take a look at this [Troubleshooting Errors during synchronization](#) and [support article](#) for guidance on how to resolve these issues.

I got an error message that my company has exceeded the number of objects that can be synchronized

- You can read more about this issue [here](#).

Other resources

- [Script to fix duplicate user principal names](#)
- [How to prepare a non-routable domain \(such as .local domain\) for directory synchronization](#)
- [Script to count total synchronized objects](#)
- [Troubleshoot AD FS 2.0](#)
- [Use PowerShell to fix empty DisplayName attributes for mail-enabled groups](#)
- [Use PowerShell to fix duplicate UPN](#)
- [Use PowerShell to fix duplicate email addresses](#)

Turn off directory synchronization for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

You can use PowerShell to turn off directory synchronization and convert your synchronized users to cloud-only. However, it is not recommended that you turn off directory synchronization as a troubleshooting step. If you need assistance with troubleshooting directory synchronization, see the [Fixing problems with directory synchronization for Microsoft 365](#) article.

[Contact support](#) for business products if needed.

Turn off directory synchronization

To turn off Directory synchronization:

1. First, install the required software and connect to your Microsoft 365 subscription. For instructions, see [Connect with the Microsoft Azure Active Directory Module for Windows PowerShell](#).
2. Use [Set-MsolDirSyncEnabled](#) to disable directory synchronization:

```
Set-MsolDirSyncEnabled -EnableDirSync $false
```

NOTE

If you use this command, you must wait 72 hours before you can turn directory synchronization back on.

Client and server software roadmap for Microsoft 365

10/28/2022 • 7 minutes to read • [Edit Online](#)

Most enterprise organizations have a heterogeneous environment that includes multiple releases of operating systems, client software, and server software. Microsoft 365 for Enterprise includes the most secure versions of the key components of your IT infrastructure. It also includes productivity features that are designed to take advantage of cloud technologies.

To maximize the business value of the Microsoft 365 for Enterprise integrated suite of products, begin planning and implementing a strategy to migrate releases of:

- The Office client installed on your computers to Microsoft 365 Apps for enterprise.
- The Office servers installed on your servers to their equivalent services in Microsoft 365.
- Windows 7 and Windows 8.1 on your devices to Windows 10 Enterprise.

NOTE

Support for Windows 7 ended on *January 14, 2020*. For more information, see the [end-of-support details](#).

As you accomplish these migrations over time, your organization comes closer to the vision of the [modern workplace](#). This secure and integrated environment can help you unlock teamwork and creativity in your organization. Microsoft 365 for Enterprise enables and empowers you all along the way.

Migration for Office client products

Organizations both large and small often use a combination of older versions of Office client products, such as Word, Excel, and PowerPoint. These older versions:

- Can be [updated](#) with the latest security updates and support fixes. But the process is sometimes manual and might not scale across your organization.
- Aren't optimized to use the Microsoft cloud technologies that help you digitally transform your business.
- Don't provide the latest features.

Microsoft 365 for Enterprise includes Microsoft 365 Apps for enterprise. This version of the Office client products is available with a Microsoft 365 for Enterprise license. It's installed and updated from the Microsoft cloud. Microsoft 365 Apps for enterprise includes security updates and the latest features. For more information, see [About Microsoft 365 Apps for enterprise](#).

Office 2007

For versions of Office in the Office 2007 release, the end of support has already passed. For more information, see [Office 2007 end-of-support roadmap](#).

Rather than upgrading your computers that run Office 2007 to Office 2010, Office 2013, or Office 2016, consider taking the following steps:

1. Get and assign a Microsoft 365 license for your users.
2. Uninstall Office 2007 on their computers.
3. Install Microsoft 365 Apps for enterprise, either individually or during an IT rollout. For more information, see [Deployment guide for Microsoft 365 Apps](#).

Microsoft 365 Apps for enterprise installs updates automatically. It can take advantage of cloud-based services for enhanced security and productivity.

Office 2010

For versions of Office in the Office 2010 release, support ended on *October 13, 2020*. For more information, see [Office 2010 end-of-support roadmap](#).

You might consider upgrading your computers that run Office 2010 to Office 2013 or Office 2016. However, both of those versions must be manually updated. So consider taking the following steps instead:

1. Get and assign a Microsoft 365 license for your users.
2. Uninstall Office 2010 on their computers.
3. Install Microsoft 365 Apps for enterprise, either individually or during an IT rollout. For more information, see [Deployment guide for Microsoft 365 Apps](#).

Microsoft 365 Apps for enterprise automatically installs both security updates and new feature updates. It can take advantage of cloud-based services in Microsoft 365 for enhanced security and productivity.

Office 2013 and Office 2016

See the [end-of-support roadmap for Office 2013](#). The end of support for Office 2016 hasn't yet been determined. In these versions, like Office 2010, you must still [install security updates](#). This task might not scale well, depending on the size of your organization.

Rather than keeping your computers current with the latest security updates for Office 2013 or Office 2016, or updating your computers from Office 2013 to Office 2016, consider taking the following steps:

1. Get and assign a Microsoft 365 license for your users.
2. Uninstall Office 2013 or Office 2016 on their computers.
3. Install Microsoft 365 Apps for enterprise, either individually or during an IT rollout. For more information, see [Deployment guide for Microsoft 365 Apps](#).

Microsoft 365 Apps for enterprise installs both security updates and new feature updates automatically. It can take advantage of cloud-based services in Microsoft 365 for enhanced security and productivity.

Migration for Office server products

Both large and small organizations often use a combination of older versions of the Office server products, such as Exchange Server and SharePoint Server. These older versions:

- Should be updated with the latest security updates and support fixes. In some cases, these updates are released monthly.
- Aren't optimized to use the Microsoft cloud technologies that help you digitally transform your business.
- Don't include new productivity applications, such as Microsoft Teams.
- Don't include the latest security features, such as Exchange and Defender for Office 365.

Microsoft 365 for Enterprise includes cloud-based versions of Office server services that use some of the same tools as on-premises versions of Office server software, such as web browsers and the Outlook client. These services are automatically updated for security. So your IT personnel save the time it takes to maintain and update on-premises servers. These services also offer new feature enhancements that aren't present in Office server software.

Use the following resources for information about migrating users and data for specific Microsoft 365 workloads:

- [Move mailboxes from on-premises Exchange Server to Exchange Online](#)
- [Migrate SharePoint data from SharePoint Server to SharePoint Online](#)

- [Migrate Skype for Business Online to Microsoft Teams](#)

Office 2007 server products

For server products in the Office 2007 release, the end of support has already passed. See these articles for details:

- [Exchange 2007 end-of-support roadmap](#)
- [SharePoint Server 2007 end-of-support roadmap](#)
- [Project Server 2007 end-of-support roadmap](#)
- [Office Communications Server end-of-support roadmap](#)
- [PerformancePoint Server 2007 end-of-support roadmap](#)

Rather than upgrading your server products in the Office 2007 release with server products in the releases for Office 2010, Office 2013, or Office 2016, consider taking the following steps:

1. Migrate the data on your Office 2007 servers to Microsoft 365. For more information or help, hire a Microsoft partner.
2. Roll out the new functionality and work processes to your users.
3. When you no longer need the on-premises servers running Office 2007 server products, decommission them.

Office 2010 server products

Support for [Exchange Server 2010](#) ended on *October 13, 2020*.

The end of support for [SharePoint Server 2010](#) is *April 13, 2021*.

Rather than upgrading these server products in the Office 2010 release with server products in the releases for Office 2013 or Office 2016, consider taking the following steps:

1. Migrate the data on your Office 2010 servers to Microsoft 365. For more information, see [FastTrack for Microsoft 365](#) or hire a Microsoft partner.
2. Roll out the new functionality and work processes to your users.
3. When you no longer need the on-premises servers running Office 2010 server products, decommission them.

Office 2013 server products

For server products in the Office 2013 release, the end of support hasn't been determined. Rather than upgrading your server products in the Office 2013 release with server products in the Office 2016 release, consider taking the following steps:

1. Migrate the data on your Office 2013 servers to Microsoft 365. For more information, see [FastTrack for Microsoft 365](#) or hire a Microsoft partner.
2. Roll out the new functionality and work processes to your users.
3. When you no longer need the on-premises servers running Office 2013 server products, decommission them.

Office 2016 server products

For server products in the Office 2016 release, the end of support hasn't been determined. To take advantage of cloud-based service and enhancements to digitally transform your business, consider taking the following steps:

1. Migrate the data on your Office 2016 servers to Microsoft 365. For more information, see [FastTrack for Microsoft 365](#) or hire a Microsoft partner.
2. Roll out the new functionality and work processes to your users.
3. When you no longer need the on-premises servers running Office 2016 server products, decommission them.

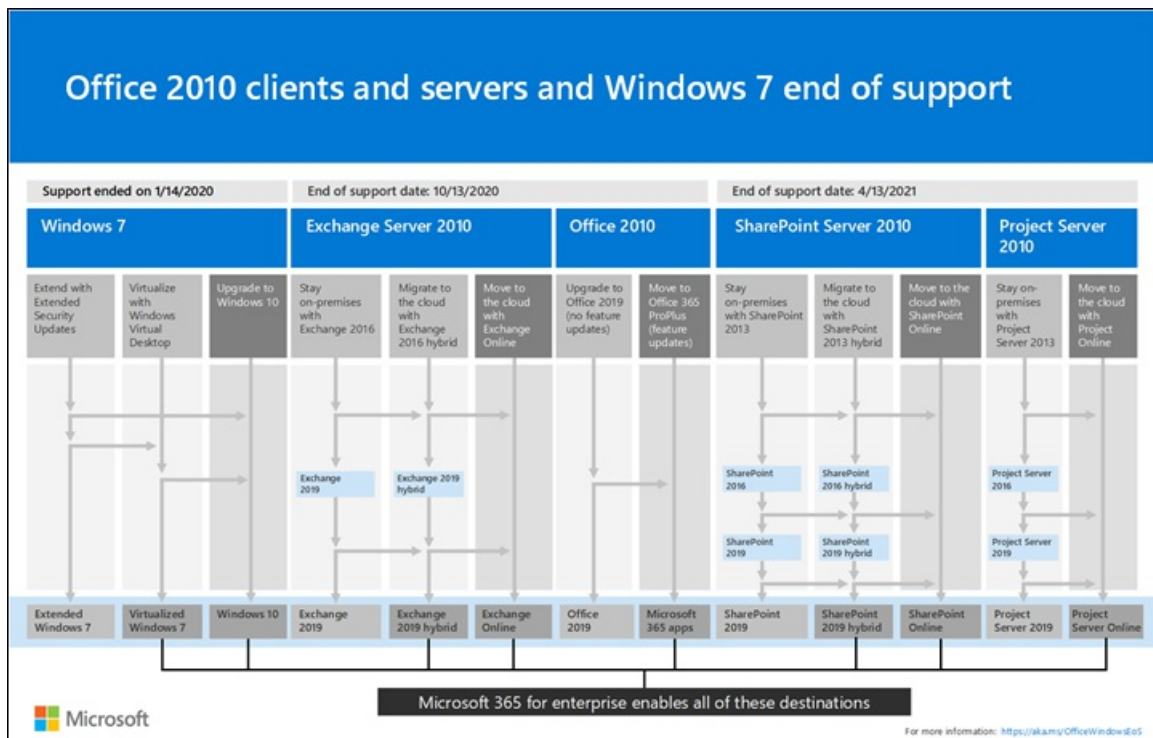
Migration for Windows 7 and 8.1

Support ended for Windows 7 on *January 14, 2020*. To migrate your devices that run Windows 7 or Windows 8.1, you can do an in-place upgrade.

For additional methods, see [Windows 10 deployment scenarios](#). You can also [plan for Windows 10 deployment](#) on your own.

Office 2010 clients and servers and Windows 7

Here's a visual summary of the upgrade, migration, and move-to-cloud options for Office 2010 clients and servers and Windows 7:



This one-page poster is a quick way to understand the paths you can take to manage the end of support for Office 2010 client and server products and Windows 7. The preferred paths are supported in Microsoft 365 for Enterprise.

You can [download this poster](#) and print it in letter size, legal size, or tabloid (11 x 17) size.

Transition your entire organization

To get a better picture of how to move your entire organization to the products and services in Microsoft 365 for Enterprise, download this transition poster:

Microsoft			
Transition Your Organization to Microsoft 365 for enterprise			
Check the boxes for what you have and follow the rows to digitally transform your business.			
From	To	Benefits	Guidance
Windows ☐ Windows 7* ☐ Windows 8.1	Windows 10	Most modern, secure Windows ever	 aka.ms/m365w10
Office client ☐ Office 2010*** ☐ Office 2013 ☐ Office 2016	Microsoft 365 Apps for enterprise	Ongoing updates include the latest features	 aka.ms/m365o365
Office servers ☐ Exchange Server 2010*** ☐ Exchange Server 2013 ☐ Exchange Server 2016	Exchange Online	Scalable, available, secure, and always up to date, with built-in compliance and information protection	 aka.ms/m365e365
☐ SharePoint Server 2010*** ☐ SharePoint Server 2013 ☐ SharePoint Server 2016	SharePoint Online	Teamwork and collaboration across your organization	 aka.ms/m365s365
☐ Lync Server 2010*** ☐ Lync Server 2013 ☐ Skype for Business Server 2015	Microsoft Teams	Real-time meetings and collaboration across your organization	 aka.ms/m365t365
* Reached end of support on January 14, 2020 ** Reached end of support on October 13, 2020 *** Reached end of support on April 13, 2021 **** With Microsoft 365 E5 or E3 with the Identity & Threat Protection offering ***** With Microsoft 365 E5 or E3 with the Information Protection & Compliance offering			
For more information, visit aka.ms/m365deploy .		© 2019 Microsoft Corporation. All rights reserved.	

This two-page poster is a quick way to inventory your existing infrastructure. Use it to get guidance for moving to a product or service in Microsoft 365 for Enterprise. It shows Windows and Office products and other infrastructure and security elements such as device management, identity and threat protection, and information and compliance protection.

How Microsoft migrated to Microsoft 365 for Enterprise

See how IT experts at Microsoft migrated the company to Microsoft 365 for Enterprise:

- [Deploying and updating Microsoft 365 Apps for enterprise](#)
- [Microsoft migrates 150,000 mailboxes to Exchange Online](#)
- [SharePoint to the cloud: Learn how Microsoft ran its own migration](#)
- [Deploying Windows 10 at Microsoft as an in-place upgrade](#)
- [Windows 10 deployment: Tips and tricks from Microsoft IT \(video\)](#)

Architectural models for SharePoint, Exchange, Skype for Business, and Lync

10/28/2022 • 6 minutes to read • [Edit Online](#)

The IT posters in this article describe the architectural models and deployment options for SharePoint, Exchange, Skype for Business, and Lync. They also provide design information for deploying SharePoint in Microsoft Azure.

By using Microsoft 365, you can provide familiar collaboration and communication services through the cloud. With a few exceptions, the user experience remains the same whether you're maintaining an on-premises deployment or using Microsoft 365.

This unified user experience complicates the decision of where to place each workload. It also raises questions:

- How do you choose a platform for individual workloads?
- Does it make sense to keep any service on-premises?
- In what scenario is a hybrid deployment appropriate?
- How does Azure fit into the picture?
- What configurations of Office server workloads does Azure support?

TIP

Most posters in this article are available in multiple languages. Available languages include Chinese, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, and Spanish. To download a poster in one of these languages, under the poster thumbnail image, select **More languages**.

Let us know what you think! Send us email at cloudadopt@microsoft.com.

Use the following links to get the posters you need:

- **Architectural models:** Use these resources to determine your ideal platform and configuration for SharePoint 2016 and Skype for Business 2015.
 - [Microsoft SharePoint 2016 architectural models](#)
 - [SharePoint Server 2016 databases](#)
 - [Microsoft Skype for Business 2015 architectural models](#)
- **Platform:** Use these resources to determine your ideal platform and configuration for SharePoint 2013, Exchange 2013, and Lync 2013.
 - [SharePoint 2013 platform options](#)
 - [Exchange 2013 platform options](#)
 - [Lync 2013 platform options](#)
- **SharePoint Server 2013 in Azure:** Use these IT posters to design and configure SharePoint Server 2013 workloads in Azure infrastructure services.
 - [Internet sites in Azure using SharePoint Server 2013](#)

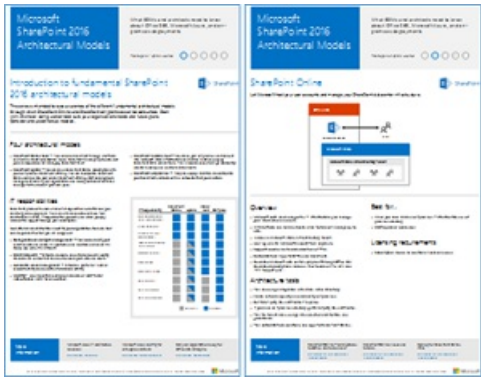
- [Design sample: Internet sites in Azure for SharePoint 2013](#)
- [SharePoint disaster recovery to Azure](#)

Architectural models posters

The IT posters for SharePoint 2016 and Skype for Business 2015 provide a way to compare deployment methods in an easy-to-print format. The posters list all configuration or platform options. They provide the following information for each option:

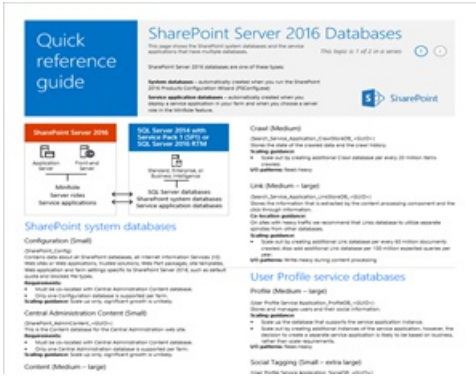
- **Overview:** A brief summary of the platform, including a conceptual diagram.
- **Best for:** Common scenarios that are ideally suited for the platform.
- **License requirements:** The licenses you need for deployment.
- **Architecture tasks:** The decisions you need to make as an architect.
- **IT pro tasks or responsibilities:** The daily responsibilities that your IT staff needs to plan for.

Microsoft SharePoint Server 2016 Architectural Models

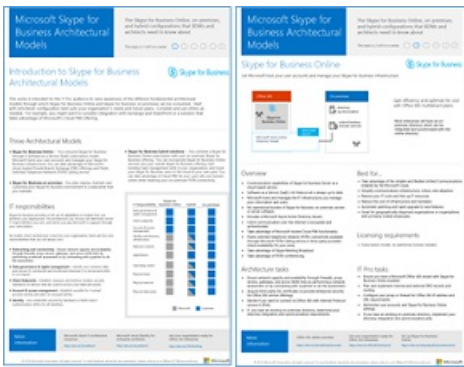
ITEM	DESCRIPTION
 PDF Visio More languages	This IT poster describes the SharePoint Online, Azure, and SharePoint on-premises configurations that business decision makers and solutions architects need to know about. - SharePoint Online (SaaS): Consume SharePoint through a software as a service (SaaS) subscription model. - SharePoint hybrid: Move your SharePoint sites and apps to the cloud at your own pace. - SharePoint in Azure (IaaS): Extend your on-premises environment into Azure, and deploy SharePoint 2016 servers there. (This model is recommended for high availability or disaster recovery environments and dev/test environments.) - SharePoint on-premises: Plan, deploy, maintain, and customize your SharePoint environment in a datacenter that you maintain.

SharePoint Server 2016 Databases

ITEM	DESCRIPTION
------	-------------

ITEM	DESCRIPTION
 PDF Visio More languages	This IT poster is a quick reference for SharePoint Server 2016 databases. You'll see details for each database: - Size - Scaling guidance - I/O patterns - Requirements The first page shows the SharePoint system databases and the service applications that have multiple databases. The second page shows all of the service applications that have single databases. For more information, see Database types and descriptions in SharePoint Server 2016.

Microsoft Skype for Business 2015 Architectural Models

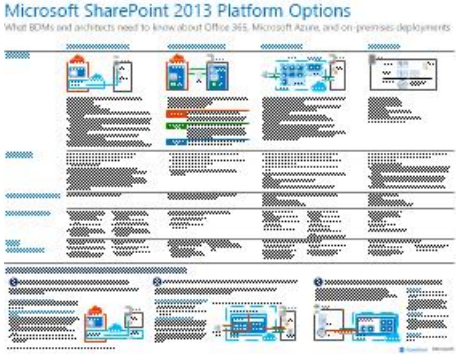
ITEM	DESCRIPTION
 PDF Visio More languages	This poster describes Skype for Business Online, on-premises, hybrid, and cloud private branch exchange (PBX). It also describes integration with Exchange and SharePoint configurations that business decision makers and solutions architects need to know about. The poster is intended for IT pros to raise awareness of the fundamental architectural models through which Skype for Business Online and Skype for Business on-premises can be consumed. Start with the configuration that best suits your organization's needs and plans. Consider and use other configurations as needed. For example, you might want to consider integration with Exchange and SharePoint or a solution that takes advantage of the Microsoft cloud PBX offering.

Platform options posters

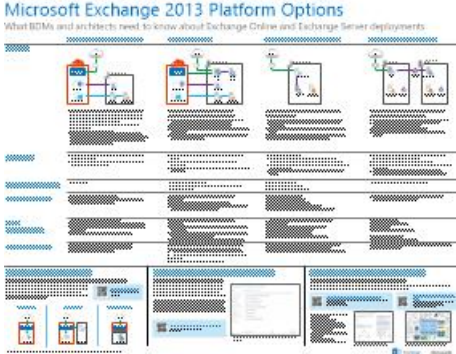
The IT posters for SharePoint 2013, Exchange 2013, and Lync 2013 provide a way to compare the deployment methods at a glance. Each poster lists all of the configurations or platform options. It provides the following information for each option:

- **Overview:** A brief summary of the platform, including a conceptual diagram.
- **Best for:** Common scenarios that are ideally suited for the platform.
- **License requirements:** The licenses you need for deployment.
- **Architecture tasks:** The decisions you need to make as an architect.
- **IT pro tasks or responsibilities:** The daily responsibilities that your IT staff needs to plan for.

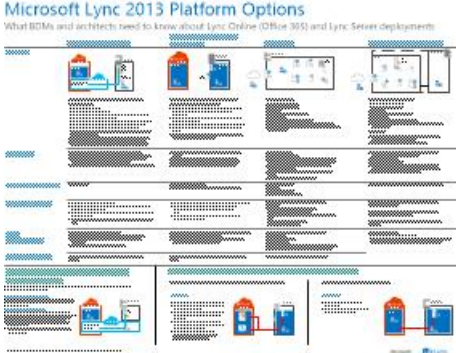
SharePoint 2013 Platform Options

ITEM	DESCRIPTION
 Microsoft SharePoint 2013 Platform Options What BDMs and architects need to know about Office 365, Microsoft Azure, and on-premises deployments PDF Visio More languages	For business decision makers and architects, this poster shows the platform options for SharePoint 2013, SharePoint in Microsoft 365, on-premises hybrid with Microsoft 365, Azure, and on-premises-only deployments. It includes an overview of each architecture, recommendations, license requirements, and lists of architect and IT pro tasks for each platform. The poster highlights several SharePoint solutions on Azure.

Exchange 2013 Platform Options

ITEM	DESCRIPTION
 Microsoft Exchange 2013 Platform Options What BDMs and architects need to know about Exchange Online and Exchange Server deployments PDF Visio More languages	For business decision makers and architects, this poster describes the platform options for Exchange 2013. Customers can choose from Exchange Online with Microsoft 365, hybrid Exchange, Exchange Server on-premises, and hosted Exchange. The poster details each architectural option, including the ideal scenarios for each, the license requirements, and IT pro responsibilities.

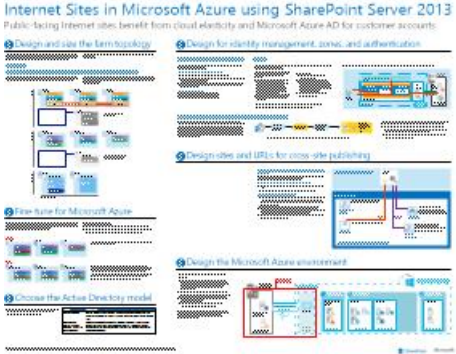
Lync 2013 Platform Options

ITEM	DESCRIPTION
 Microsoft Lync 2013 Platform Options What BDMs and architects need to know about Lync Online (Office 365) and Lync Server deployments PDF Visio More languages	For business decision makers and architects, this poster describes the platform options for Lync 2013. Customers can choose from Lync Online with Microsoft 365, hybrid Lync, Lync Server on-premises, and hosted Lync. The IT poster details each architectural option, including the ideal scenarios for each, the license requirements, and IT pro responsibilities.

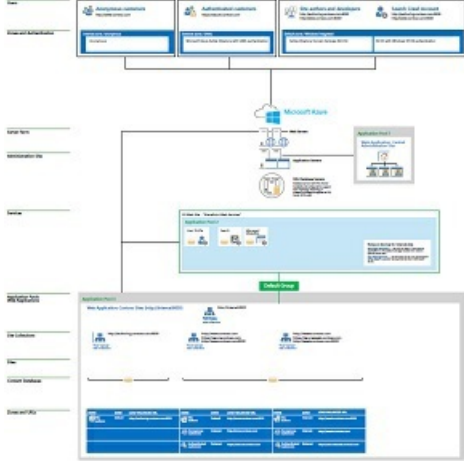
SharePoint in Azure solutions posters

The IT posters for SharePoint in Azure show Azure-based solutions that use SharePoint Server 2013.

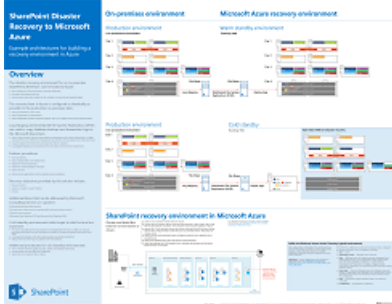
Internet Sites in Microsoft Azure Using SharePoint Server 2013

ITEM	DESCRIPTION
Internet Sites in Microsoft Azure using SharePoint Server 2013 Public-facing Internet sites benefit from cloud identity and Microsoft Azure AD for customer accounts.  PDF Visio More languages	This poster outlines key design activities and recommended architecture for internet-facing sites in Azure. For more information, see the following articles: - Internet sites in Azure using SharePoint Server 2013 - Azure architectures for SharePoint 2013

Internet sites in Azure for SharePoint 2013

ITEM	DESCRIPTION
Internet sites in Microsoft Azure for SharePoint Server 2013  PDF Visio More languages	Use this design sample as a starting point for your own architecture of an internet-facing site in Azure using SharePoint Server 2013. For more information, see the following articles: - Internet sites in Azure using SharePoint Server 2013 - Azure architectures for SharePoint 2013

SharePoint Disaster Recovery to Microsoft Azure

ITEM	DESCRIPTION
SharePoint Disaster Recovery to Microsoft Azure On-premises environment Microsoft Azure recovery environment  PDF Visio More languages	This IT poster shows architecture principles for a disaster recovery environment in Azure. For more information, see the following articles: - SharePoint Server 2013 disaster recovery in Azure - Azure architectures for SharePoint 2013

See also

- [Microsoft 365 solution and architecture center](#)
- [Microsoft cloud architecture models](#)

- [Microsoft 365 test lab guides](#)
- [Hybrid solutions](#)

Plan your upgrade from Office 2007 or Office 2010 servers and clients

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 for Enterprise and Office 365 for Enterprise.

If your organization uses old versions of Office products and servers, now is a great time to start planning your upgrade. Office 2007 products and services have reached their [end of support](#). For Office 2010 products and services:

- Office 2010 and Exchange 2010 reached their end of support on *October 13, 2020*.
- SharePoint 2010 and Project Server 2010 will reach their end of support on *April 13, 2021*.

For more information, see [Upgrade from Office 2010 servers and clients](#).

Use the resources in this article to get started on your upgrade.

What is Microsoft 365?

[Microsoft 365](#) is a combination of innovative Office apps, intelligent cloud services, and world-class security that's designed to help you achieve more.

Microsoft 365 includes the licenses and capabilities to help ensure that your organization is working on the latest Windows operating system. It also ensures that your Windows, iOS, and Android devices are enrolled with and secured by policies that require authentication and data protection. Additionally, Windows 10 and your Microsoft 365 Apps for Enterprise (previously named Office 365 ProPlus) client software is continually updated to include the latest features and security updates.

Microsoft 365 is the way to digitally transform your business with constantly improving devices and productivity experiences that are enabled and secured by the Microsoft cloud.

RESOURCE	DESCRIPTION
Microsoft 365	Get information about the versions of Microsoft 365.
Microsoft 365 for Business documentation	Get detailed information about the version of Microsoft 365 for small and medium businesses.
Microsoft 365 for Education documentation	Get detailed information about the version of Microsoft 365 for educational organizations.
Microsoft 365 for Enterprise documentation	Get detailed information about the version of Microsoft 365 for enterprise organizations.

What happens if I don't upgrade?

You can choose not to upgrade at this time. Your on-premises servers and applications will continue to run. But when you no longer receive security updates or support options, your organization could be vulnerable to security breaches. We strongly recommend that you plan your upgrade soon. You can upgrade to Microsoft 365 or to newer versions of your on-premises servers and applications.

What upgrade options are available?

Organizations should consider several upgrade options:

- **Upgrade your on-premises servers and applications.** If you're using Office products and server applications on-premises, see the following planning content:

OFFICE 2007 PRODUCTS AND SERVICES	OFFICE 2010 PRODUCTS AND SERVICES
Office 2007 (Desktop)	Office 2010 (Desktop)
Exchange 2007	Exchange 2010
SharePoint 2007	SharePoint 2010
Office Communications Server	Lync Server 2010
Project Server 2007	Project Server 2010
PerformancePoint Server 2007	

- **Implement a hybrid solution with Microsoft 365 or Office 365.** A hybrid solution uses your on-premises servers and applications and their cloud equivalents. If you're moving to the cloud in phases or you must keep some server and applications on-premises, a hybrid solution might be right for your organization. For more information, see [Microsoft cloud architecture models](#).
- **Move to the cloud with Microsoft 365 or Office 365.** For many customers, moving to the cloud is an efficient and cost-effective solution. A complete move to the cloud makes setup and ongoing management easier. This option seamlessly provides all the latest features and security updates. For more information, see the [What is Microsoft 365?](#) section in this article.

Can I get help for my organization?

If you want help with planning your upgrade, consider one or more of the following options:

- Work with a partner or volume licensing specialist. [Find your Microsoft 365 partner or reseller](#).
- If your organization purchases a qualifying number of Microsoft 365 licenses, our FastTrack team can help you through the setup process. For more information, see [FastTrack for Microsoft 365](#).
- If you're part of a small organization, or if you prefer to handle your organization's Office upgrade yourself, see [Upgrade your Microsoft 365 Business users to the latest Office client](#).

I'm a home user. What do I do?

If you're using Office 2007 or Office 2010 at home, consider the following upgrade options:

- **Use Office in a browser for free.** Create, view, and edit Office files in your browser. Get access to those files from just about any device that has internet access.

[Office on the web](#) includes [Word for the web](#), [Excel for the web](#), [PowerPoint for the web](#), [OneNote for the web](#), [Sway](#), [Email](#), [Calendar](#), and [OneDrive](#). To get started, visit [Office.com](#) and sign in by using your [Microsoft account](#). If you don't have a Microsoft account, you can create one at [Office.com](#).

- **Try Microsoft 365 Family.** Start a trial of [Microsoft 365 Family](#) to see how it works for you. With Microsoft 365 Family, you'll enjoy cloud storage with OneDrive.

Support for Windows 7 [ended on January 14, 2020](#). The versions of Word, Excel, PowerPoint, Outlook, Publisher, and Access that are provided with Office 365 Home or Office 365 Personal and that run on Windows 7 devices receive security updates but not feature updates. To continue receiving feature updates for these applications, [upgrade your Windows 7 devices to Windows 10](#).

- **Purchase Office Home & Student.** If you choose this option, you make a one-time purchase and then install Office on your Windows PC or Mac. This purchase isn't a subscription; it's a one-time, perpetual-use license for one computer. View the [requirements](#) and then choose a version.
 - If your Windows PC is running Windows 10, consider getting [Office Home & Student 2019](#).
 - If your Windows PC is running Windows 7, 8, or 8.1 and you're not upgrading to Windows 10 now, consider getting Office Home & Student 2016 or another edition of Microsoft Office. You can get it from an authorized reseller.

Support for Windows 7 [ended on January 14, 2020](#). Microsoft no longer provides security updates for it. Upgrade your Windows 7 devices to Windows 10 for continued security and feature updates and ongoing support.

If you choose not to upgrade now, your Office apps will continue to run according to the [timelines](#). However, to get security updates or new and improved features, you need to upgrade.

Next steps

- [Upgrade from Office 2007 servers and clients](#)
- [Upgrade from Office 2010 servers and clients](#)

Related topics

[Microsoft Lifecycle Policy](#)

Resources to help you upgrade from Office 2013 clients and servers

10/28/2022 • 2 minutes to read • [Edit Online](#)

If you're using Office 2013 clients and servers, be aware that **support ends on April 11, 2023**. If you haven't already begun to upgrade from them to newer versions, we recommend you start now.

As you plan your upgrade, consider moving to Microsoft 365.

- Microsoft 365 has cloud-based services, such as Exchange Online, SharePoint, and Teams.
- Microsoft 365 Apps for enterprise provides Office client apps that you can install on local devices. The apps are updated regularly from the Microsoft cloud with new productivity and security features.

Upgrade planning resources

The following table provides links to planning resources to help you upgrade from these Office 2013 clients and servers.

PRODUCT	PLANNING RESOURCE
Office 2013 (desktop apps) Project 2013 Visio 2013	Plan an upgrade from older versions of Office to Microsoft 365 Apps
Exchange Server 2013	Exchange 2013 end of support roadmap
SharePoint Server 2013 SharePoint Foundation 2013	Upgrading from SharePoint 2013
Project Server 2013	Project Server 2013 end of support roadmap
Lync Server 2013	Upgrading from Lync Server 2013

We also recommend business and enterprise customers use the deployment benefits provided by Microsoft and Microsoft Certified Partners, including [Microsoft FastTrack](#) for cloud migrations.

NOTE

If you use Office 2013 products and applications at home, [review this information](#) for your upgrade choices.

Related articles

- [Microsoft Lifecycle Policy](#)
- [Plan your upgrade from Office 2007 or Office 2010 servers and clients](#)

Exchange 2013 end of support roadmap

10/28/2022 • 11 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Exchange Server 2013 will reach its end of support on **April 11, 2023**. If you haven't already begun your migration from Exchange 2013 to Microsoft 365, Office 365, or Exchange 2019, now's the time to start planning.

What does *end of support* mean?

Most Microsoft products have a support lifecycle during which they get new features, bug fixes, security fixes, and so on. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. Because Exchange 2013 reaches its end of support on April 11, 2023, Microsoft will no longer provide the following after this date:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

Your installation of Exchange 2013 will continue to run after this date. But because of the changes listed above, we strongly recommend that you migrate from Exchange 2013 to Exchange 2019 as soon as possible.

What are my options?

It's a great time to explore your options and prepare a migration plan. You can:

- Migrate to Microsoft 365. Migrate mailboxes, public folders, and other data using cutover, minimal hybrid, or full hybrid migration. Then, remove on-premises Exchange servers and Active Directory.
- Upgrade Exchange 2013. Move to Exchange 2019 for your on-premises servers.

IMPORTANT

If your organization chooses to migrate mailboxes to Microsoft 365 but plans to keep using Azure AD Connect to manage user accounts in Active Directory, you need to keep at least one Microsoft Exchange server on-premises. If you remove all Exchange servers, you won't be able to make changes to Exchange recipients in Exchange Online because the source of authority is your on-premises Active Directory. In this scenario, you have the following options:

- *Recommended:* Migrate your mailboxes to Microsoft 365 and upgrade your environment to Exchange 2019 by April 11, 2023. Use Exchange 2013 to connect to Microsoft 365 and migrate mailboxes. Next, upgrade from Exchange 2013 to Exchange 2019, and decommission servers running Exchange 2013.
- If you can't complete a migration to Exchange Online and upgrade your on-premises servers by April 11, 2023, upgrade from Exchange 2013 to Exchange 2019 first and then use Exchange 2019 to migrate mailboxes to Microsoft 365.

Here are the three paths you can take to avoid the end of support for Exchange Server 2013.

Migrate to Microsoft 365

Migrating to Microsoft 365 is the best and simplest option to help you retire your Exchange 2013 deployment. With a migration to Microsoft 365, you can make a single hop from old technology to current features,

including:

- Larger mailboxes with greater data resilience;
- Security capabilities such as anti-spam and antimalware protection,
- Compliance capabilities such as Data Loss Prevention, Retention Policies, In-Place and Litigation Hold, in-place eDiscovery, and more;
- Integration with SharePoint Online, OneDrive, Teams, Power BI, and other Microsoft 365 services;
- Focused Inbox; and
- Advanced analytics and Viva Insights.

Microsoft 365 also gets new features and experiences first, so your organization can start using them right away. Also, you won't have to worry about:

- Purchasing and maintaining hardware;
- Paying to run and cool your servers;
- Keeping servers up to date on security, product, and time-zone fixes;
- Maintaining server storage and software to support compliance requirements; or
- Upgrading to a new version of Exchange; you're always on the latest version with Microsoft 365.

How should I migrate to Microsoft 365?

Depending on your organization, you have a few options to get to Microsoft 365. First, you need to consider a few things, such as:

- The number of mailboxes you need to move;
- How long you want the migration to last; and
- Whether you need a seamless integration between your on-premises environment and Microsoft 365 during the migration.

This table shows your migration options and the most important factors that determine which method to use.

MIGRATION OPTION	ORGANIZATION SIZE	DURATION
Cutover migration	Fewer than 150 mailboxes	A week or less
Minimal hybrid migration	Fewer than 150 mailboxes	A few weeks or less
Full hybrid migration	More than 150 mailboxes	A few weeks or more

The following sections give you an overview of these methods. For more information, see [Decide on a migration path](#).

Cutover migration

In a cutover migration, you migrate all your mailboxes, distribution groups, contacts, and so on, to Office 365 at a set date and time. When you're done, you shut down your on-premises Exchange servers and start using Microsoft 365 exclusively.

Cutover migration is great for small organizations that don't have many mailboxes, want to get to Microsoft 365 quickly, and don't want to deal with the complexity of the other methods. But it should be completed in a week or less. And it requires users to reconfigure their Outlook profiles. Cutover migration can migrate up to 2,000 mailboxes, but we recommend you use it for a maximum of 150. If you try to migrate more, you could run out of time to transfer all the mailboxes before your deadline, and your IT support staff may get overwhelmed with

requests to help users reconfigure Outlook.

Here are things to consider about cutover migration:

- Microsoft 365 will need to connect to your Exchange 2013 servers by using Outlook Anywhere over TCP port 443.
- All on-premises mailboxes will be moved to Microsoft 365.
- You'll need an on-premises administrator account that has read access to your users' mailboxes.
- The Exchange 2013 accepted domains that you want to use in Microsoft 365 need to be added as verified domains in the service.
- Between when you start the migration and when you begin the completion phase, Microsoft 365 will periodically synchronize the Microsoft 365 and on-premises mailboxes. This lets you complete the migration without worrying about email being left behind in your on-premises mailboxes.
- Users will receive new temporary passwords for their Microsoft 365 account. They'll need to change those when they sign in to their mailboxes for the first time.
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users will need to set up a new Outlook profile on each of their devices and download their email again. The amount of email that Outlook will download can vary. For more information, see [Work offline in Outlook](#).

To learn more about cutover migration, see:

- [What you need to know about a cutover email migration](#)
- [Perform a cutover migration of email to Office 365](#)

Minimal hybrid migration

In a minimal hybrid, or express, migration you move a few hundred mailboxes to Microsoft 365 within a few weeks. This method doesn't support advanced hybrid-migration features like shared free/busy calendar information.

Minimal hybrid migration is great for organizations that need to take more time to migrate their mailboxes to Microsoft 365, but still plan to complete the migration within a few weeks. You get some of the benefits of the more advanced *full-hybrid migration* without much of the complexity. You can control how many and which mailboxes to migrate at a given time. Microsoft 365 mailboxes will be created with the user names and passwords of the on-premises accounts. And, unlike cutover migrations, your users don't have to recreate their Outlook profiles.

Here are things to consider about minimal hybrid migration:

- You'll need to do a one-time directory synchronization between your on-premises Active Directory servers and Microsoft 365.
- Users will be able to sign in to their Microsoft 365 mailbox with the same user name and password as before their mailbox.
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox that you migrate.
- Users won't need to set up a new Outlook profile on most of their devices, though some older Android phones might need a new profile. Users won't need to redownload their email.

For more information, see [Use Minimal Hybrid to quickly migrate Exchange mailboxes to Office 365](#).

Full hybrid

In a full hybrid migration, you have many hundreds, up to tens of thousands, of mailboxes, and you move some or all to Microsoft 365. Because these migrations are typically longer-term, hybrid migrations make it possible to:

- Show on-premises users the free/busy calendar information for users in Microsoft 365, and vice versa.
- See a unified global address list that contains recipients in both on-premises and Microsoft 365.

- View full Outlook recipient properties for all users, regardless of whether they're on-premises or in Microsoft 365.
- Secure email communication between on-premises Exchange servers and Office 365 using TLS and certificates.
- Treat messages sent between on-premises Exchange servers and Microsoft 365 as internal, enabling them to:
 - Be properly evaluated and processed by transport and compliance agents targeting internal messages.
 - Bypass anti-spam filters.

Full hybrid migrations are best for organizations that expect to stay in a hybrid configuration for many months or more. You get the features listed earlier in this section, plus directory synchronization, better integrated compliance features, and the ability to move mailboxes to and from Microsoft 365 using online mailbox moves. Microsoft 365 becomes an extension of your on-premises organization.

Things to consider about full-hybrid migration:

- They aren't suited to all organizations. Due to the complexity of full hybrid migrations, organizations with less than a few hundred mailboxes don't typically see benefits that justify the effort and cost involved. In such cases, we recommend that you consider cutover or minimal hybrid migration instead.
- You need to set up directory synchronization using Azure Active Directory (Azure AD) Connect between your on-premises Active Directory servers and Microsoft 365.
- Users will be able to sign in to their Microsoft 365 mailbox with same user name and password they use when they sign in to the local network. (This functionality requires Azure AD Connect with password synchronization and/or Active Directory Federation Services).
- You need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users don't need to set up a new Outlook profile on most of their devices, although some older Android phones might need a new profile. Users won't need to redownload their email.

IMPORTANT

If your organization chooses to migrate mailboxes to Microsoft 365 but plans to keep Azure AD Connect to manage user accounts in Active Directory, you need to keep at least one Exchange server on-premises. If all Exchange servers are removed, you won't be able to make changes to Exchange recipients. This is because the source of authority is Active Directory and changes need to be made there.

If a full hybrid migration sounds right for you, see the following helpful resources:

- [Exchange Deployment Assistant](#)
- [Exchange Server Hybrid Deployments](#)
- [Hybrid Configuration wizard](#)
- [Hybrid Configuration wizard FAQs](#)
- [Hybrid deployment prerequisites](#)

Upgrade to a newer version of Exchange Server on-premises

We strongly believe that you get the best value and user experience by migrating fully to Microsoft 365. But we understand that some organizations need to keep some Exchange servers on-premises. This might be because of regulatory requirements, to guarantee data isn't stored in a foreign datacenter, because you have unique settings or requirements that can't be met in the cloud, or because you need Exchange to manage cloud mailboxes because you still use Active Directory on-premises. In any case, if you keep Exchange on-premises, you should ensure your Exchange 2013 environment is upgraded.

For the best experience, we recommend that you upgrade your remaining on-premises environment to

Exchange 2019. You don't need to install Exchange Server 2016 because you can go directly from Exchange Server 2013 to Exchange Server 2019. Exchange 2019 most closely matches the experience available with Microsoft 365, although some features are available only in Microsoft 365.

Below are important things to know about upgrading Exchange 2013:

ITEM	MORE INFORMATION
End of support dates	Like Exchange 2013, each version of Exchange has its own end-of-support date: Exchange 2013 - April 2023 April 2023 is a lot closer than you think!
Migration path to Exchange 2019	The migration path from Exchange 2013 to a newer version is simple: Install Exchange 2019 into your existing Exchange 2013 organization. Move services and data from Exchange 2013 to Exchange 2019 and decommission Exchange 2013 servers.
Server hardware	Server hardware requirements have changed from Exchange 2013. Make sure your hardware is compatible. Find out more about hardware requirements here: Exchange 2019 system requirements With the significant improvements in Exchange performance and the increased computing power and storage capacity in newer servers, you'll likely need fewer servers to support the same number of mailboxes.
Operating system version	The minimum supported operating system version for Exchange 2019 is Windows Server 2019. Windows Server 2022 support is coming soon You can find more information about operating system support at Exchange Supportability Matrix .
Active Directory forest functional level	The minimum supported Active Directory forest functional level is Windows Server 2012 R2. You can find more information about forest functional level support at Exchange Supportability Matrix .
Office client versions	The minimum supported Office client version is also documented in the Exchange Supportability Matrix .

Use the following resources to help with your migration:

- [Exchange Deployment Assistant](#)
- Active Directory [schema changes for Exchange 2019](#)
- System [requirements for Exchange 2019](#)

What if I need help?

If you're migrating to Microsoft 365, you might be eligible to use our Microsoft FastTrack service. FastTrack

provides best practices, tools, and resources to make your migration to Microsoft 365 as seamless as possible. Best of all, you'll have a support engineer walk you through from planning and design to migrating your last mailbox. For more about FastTrack, see [Microsoft FastTrack](#).

If you run into problems during your migration to Microsoft 365 and you aren't using FastTrack, or you're migrating to a newer version of Exchange Server, here are some resources you can use:

- [Technical community](#)
- [Customer support](#)

Upgrading from SharePoint 2013

10/28/2022 • 4 minutes to read • [Edit Online](#)

Both Microsoft SharePoint Server 2013 and SharePoint Foundation 2013 will reach end of support on **April 11, 2023**. This article provides resources to help you migrate your existing SharePoint Server data to SharePoint Online in Microsoft 365 or upgrade your on-premises SharePoint 2013 environment. For the rest of this article, we'll use SharePoint 2013 to refer to both SharePoint Server 2013 and SharePoint Foundation 2013.

What is *end of support*?

Most Microsoft products have a support lifecycle, during which they get new features, bug fixes, security fixes, and so on. After the end-of-support date, the product doesn't stop working, but Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

That means there will be no further updates, patches, or fixes for the product (including security patches/fixes). Microsoft Support will have fully shifted its support efforts to more recent versions.

NOTE

A software lifecycle typically lasts for five years of mainstream support from the initial release, and potentially up to an additional 5 years of extended support. [Microsoft solution providers](#) can help you upgrade to the next version of the software or migrate to Microsoft 365 (or both). Make sure you're aware of end-of-support dates for critical underlying technologies as well, particularly for the version of Microsoft SQL Server you're using with SharePoint. For more information, see [Fixed Lifecycle Policy](#).

Plan ahead

Check the dates that support ends on the Product Lifecycle site for [SharePoint Server 2013](#) and [SharePoint Foundation 2013](#). Plan your upgrades or migrations with these dates in mind. Remember that your product *won't stop working* at the date listed. But because your installation will no longer be patched after that date, you'll want to plan a smooth transition to the next version of the product. The table below lists the options available to you.

END OF SUPPORT PRODUCT	GOOD	BETTER	BEST
SharePoint Server 2013 SharePoint Foundation 2013	Upgrade to SharePoint Server 2016 or 2019	Upgrade to SharePoint Server Subscription Edition	Migrate to SharePoint in Microsoft 365

What's next?

We recommend migrating to SharePoint in Microsoft 365 to take advantage of the latest collaboration, intelligence, and security solutions in Microsoft 365. The modern experience features in Microsoft 365 are

designed to be compelling, flexible, and performant.

If you have a need to maintain an on-premises SharePoint deployment, we recommend a hybrid deployment that will enable you to migrate as much of SharePoint functionality as you can to SharePoint in Microsoft 365. See [SharePoint hybrid](#) to learn about and plan for a hybrid implementation.

Migrate to SharePoint in Microsoft 365

You can use the SharePoint Migration Tool (SPMT) to migrate your sites and content to SharePoint in Microsoft 365. We have an extensive library of content that can help you plan ahead, perform your migration, and troubleshoot any issues you may come across. [Overview of the SharePoint Migration Tool](#) is a good place to start.

Upgrade to SharePoint Server Subscription Edition

Even though there isn't a direct path to upgrade from SharePoint 2013 to the Subscription Edition, this still is the second best option. The primary reason is that SharePoint Server Subscription Edition introduces a continuous update model that eliminates the need to release new major versions of SharePoint Server going forward.

To upgrade to Subscription Edition, you must be running SharePoint Server 2016 or 2019. Since there also isn't a direct path from SharePoint 2013 to 2019 either, your best option is to upgrade to 2016 first and then upgrade to Subscription Edition. See the links below to learn more about and plan your upgrade to Subscription Edition:

- [Upgrade to SharePoint Server 2016](#)
- [Upgrade to SharePoint Server Subscription Edition](#)

Even if you have a need to maintain an on-premises SharePoint deployment, we recommend that you migrate parts of your sites or content to Microsoft 365 with [SharePoint hybrid](#) implementation to start taking advantage of the modern collaboration experiences, security and compliance features in Microsoft 365.

Upgrade to SharePoint Server 2016 or 2019

Both SharePoint Server 2016 and 2019 are supported platforms if you plan to maintain your on-premises SharePoint deployment beyond the end of support for 2013. However, **both versions will reach end of support on July 14, 2026**. This means that you will need to plan another upgrade within 3 years after the end of support date for 2013. Here are the support lifecycle pages for both products:

- [SharePoint Server 2016 support lifecycle dates](#)
- [SharePoint Server 2019 support lifecycle dates](#)

To learn more and plan your upgrade, see the following articles:

- [Upgrade to SharePoint Server 2016](#)
- [Upgrade to SharePoint Server 2019](#)

Even if you have a need to maintain an on-premises SharePoint deployment, we recommend that you migrate parts of your sites or content to Microsoft 365 with [SharePoint hybrid](#) implementation to start taking advantage of the modern collaboration experiences, security and compliance features in Microsoft 365.

Upgrading from Lync Server 2013

10/28/2022 • 3 minutes to read • [Edit Online](#)

Microsoft Lync Server 2013 will reach end of support on **April 11, 2023**. This article provides resources to help you upgrade your existing Lync Server deployment to Microsoft Teams or Skype for Business on-premises.

What is *end of support*?

Most Microsoft products have a support lifecycle, during which they get new features, bug fixes, security fixes, and so on. After the end-of-support date, the product doesn't stop working, but Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

That means there will be no further updates, patches, or fixes for the product (including security patches/fixes). Microsoft Support will have fully shifted its support efforts to more recent versions.

Plan ahead

Check the dates that support ends on the [Product Lifecycle site](#). Plan your upgrades or migrations with these dates in mind. Remember that your product *won't stop working* at the date listed. But because your installation will no longer be patched after that date, you'll want to plan a smooth transition to the next version of the product. The table below lists the options available to you.

END OF SUPPORT PRODUCT	SUPPORTED	RECOMMENDED
Lync Server 2013	Upgrade to Skype for Business Server 2015 or 2019	Upgrade to Microsoft Teams

What's next?

We recommend upgrading to Microsoft Teams. Microsoft Teams extends the capabilities of Lync Server, bringing together chat, meetings, calling, collaboration, app integration, and file storage into a single interface. Teams helps streamline the way users get things done, improving user satisfaction and accelerating business outcomes. We're continually expanding Teams' capabilities to enable you to communicate and collaborate in new ways, break down organizational and geographical barriers, and drive efficiency in process and decision making.

If you can't upgrade to Microsoft Teams, you can upgrade to Skype for Business Server 2015 or 2019. A key planning consideration to know is that both of these products will reach end of support on October 14, 2025. For more information, see the following support lifecycle pages:

- [Skype for Business Server 2015 support lifecycle information](#)
- [Skype for Business Server 2019 support lifecycle information](#)

Upgrade to Microsoft Teams

We have detailed guidance on upgrading to Microsoft Teams from your on-premises deployment. First, let's

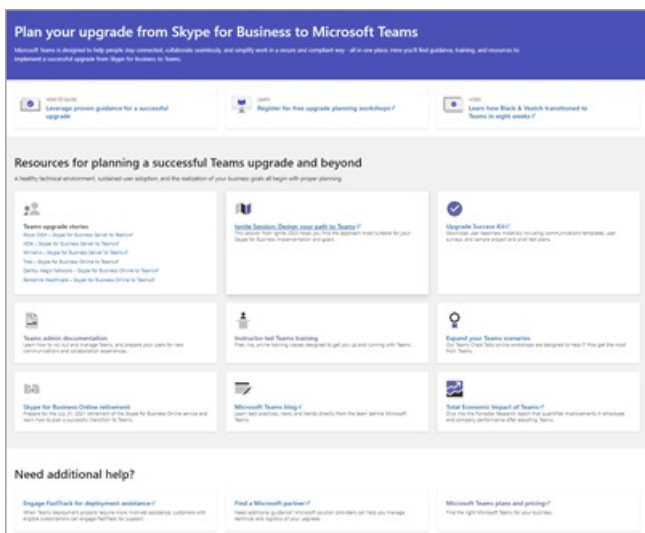
cover some key technical requirements. You will need to establish hybrid connectivity, which will enable you to move your users to Teams. [Plan hybrid connectivity](#) gives an overview of setting up a hybrid environment. Even though the article is focused on Skype for Business, all the concepts apply to Lync Server 2013 as well. See the [server version requirements](#) section for Lync Server 2013-specific details.

You also need to ensure that your Lync Server 2013 deployment is fully up to date. We publish a [list of all the latest updates for Lync Server 2013](#) However, the following update is a pre-requisite for an upgrade to Microsoft Teams:

- [September 2021 cumulative update 5.0.8308.1149 for Lync Server 2013, Core Components](#): This update replaces the Live ID authentication with OAuth authentication protocol for the `Move-CSUser` cmdlet, which is used for moving on-premises users to Microsoft Teams.

Even though the user experience in Microsoft Teams is far richer and superior to Lync, it is also dramatically different. Therefore, you'll also need to prepare your organization and your users to ensure a rapid adoption of Microsoft Teams. We have a wealth of information available on how to prepare your organization, plan your upgrade to Teams, and ensure a successful rollout.

We recommend that you start at our [Teams upgrade portal](#) where you can find technical information, training resources, links to Ignite sessions, available help resources, case studies and more.



Upgrade to Skype for Business Server

The path to Skype for Business Server is going to be different depending on the version you choose to upgrade to. Skype for Business Server 2015 supports an in-place upgrade from Lync Server 2013. On the other hand, in order to upgrade to Skype for Business Server 2019, you first will need to introduce Skype for Business Server 2019 to your Lync Server 2013 installation via adding one or more new servers, and then transfer operations to the new 2019 servers you've added.

One important point to consider is that the current support phase for each product: Skype for Business 2019 is in mainstream support and Skype for Business 2015 is currently in extended support. Therefore, we recommend upgrading to Skype for Business Server 2019. To learn more about the difference between mainstream and extended support, see [Fixed Lifecycle Policy](#).

See the following resources for detailed information about each upgrade scenario.

- Upgrade to Skype for Business Server 2019
- Upgrade to Skype for Business Server 2015

Project Server 2013 end of support roadmap

10/28/2022 • 5 minutes to read • [Edit Online](#)

Project Server 2013 will reach end of support on **April 11, 2023**. If you're currently using Project Server 2013, note that Project 2013 desktop app also has the same end-of-support dates.

What does *end of support* mean?

Almost all Microsoft products have a support lifecycle, during which they get new features, bug fixes, and security updates. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. After Project Server 2013 reaches its end of support on April 11, 2023, Microsoft will no longer provide:

- Technical support for problems that may occur.
- Bug fixes for issues that are discovered and that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that are discovered and that may make the server vulnerable to security breaches.
- Time zone updates.

Your installation of Project Server 2013 will continue to run after this date. But, because of the changes listed previously, we strongly recommend that you migrate from Project Server 2013 as soon as possible.

What are my options?

Your migration options are:

- Migrate to Project Online
- Migrate to a newer on-premises version of Project Server (preferably Project Server Subscription Edition)

WHY WOULD I PREFER TO MIGRATE TO PROJECT SERVER 2019?	WHY WOULD I PREFER TO MIGRATE TO PROJECT ONLINE?
Business rules restrict me from operating my business in the cloud. I need control of updates to my environment.	I have mobile or remote users. Costs to migrate on-premises servers are a significant concern (hardware, software, time and effort to implement, and so on). After migration, costs to maintain my environment are a concern (for example, automatic updates, guaranteed uptime, and so on).

NOTE

Project Server doesn't support hybrid configuration because Project Server and Project Online can't share the same resource pool.

Important considerations for migrating from Project Server 2013

Consider the following when you plan to migrate from Project Server 2013:

- **Get help from a Microsoft solution provider** - An upgrade from Project Server 2013 can be a challenge. It requires much preparation and planning. It can be especially challenging if you weren't the person who originally set up Project Server 2013. Microsoft solution providers are available to help, whether you plan to migrate to Project Server Subscription Edition or to Project Online. Search for a solution provider in the [Microsoft solution provider center](#).
- **Time and patience** - Upgrade planning, execution, and testing will take considerable time and effort, especially for an upgrade to Project Server Subscription Edition. If you're migrating from Project Server 2013 to Project Server Subscription Edition, you must first migrate to Project Server 2016, check your data, and then to Project Server Subscription Edition. You might want to check with a Microsoft solution provider for a time frame and estimated cost for them to assist.

Migrate to Project Online

If you choose to migrate from Project Server 2013 to Project Online, you can follow these steps to manually migrate your project plan data:

1. Save your project plans from Project Server 2013 to .mpp format.
2. Using Project Professional 2016, Project Professional 2019, or the Project Online Desktop Client, open each .mpp file, and then save and publish it to Project Online.

You can manually create your PWA configuration in Project Online (for example, recreate any needed custom fields or enterprise calendars). Microsoft solution providers can also help with this process.

Key resources:

RESOURCE	DESCRIPTION
Get started with Project Online	How to set up and use Project Online
Project Online Service Description	Information about the different Project Online plans available

Migrate to a newer on-premises version of Project Server

We strongly believe that you get the best value and user experience by migrating to Project Online. But we also understand some organizations need to keep project data on-premises. If you choose to keep your project data on-premises, you can migrate your Project Server 2013 environment to Project Server 2016, Project Server 2019, or Project Server Subscription Edition.

If you can't migrate to Project Online, we recommend that you migrate to Project Server Subscription Edition which includes most of the key features in previous releases of Project Server. And it most closely matches the experience available with Project Online, although some features are available only in Project Online. Additional factors to consider are:

- Project Server Subscription Edition introduces a continuous update model that eliminates the need to release new major versions of Project Server going forward.
- Both Project Server 2016 and 2019 will reach end of support on July 14, 2026. If you migrate to either version, you will need to plan for another upgrade within three years. For more information, see the support lifecycle pages for both [2016](#) and [2019](#).

After you complete each migration, make sure that your data migrated successfully.

How do I migrate to Project Server Subscription Edition?

The architectural differences between Project Server 2013 and Project Server Subscription Edition prevent a direct migration path. So you'll need to migrate your Project Server 2013 data first to Project Server 2016, and then to Project Server Subscription Edition.

1. Migrate to Project Server 2016.
2. Migrate from Project Server 2016 to Project Server Subscription Edition.

After you complete each migration, make sure that your data migrated successfully.

Step 1: Migrate to Project Server 2016

For a comprehensive information about upgrading from Project Server 2013 to Project Server 2016, see [Upgrade to Project Server 2016](#).

Key resources:

- [Overview of the Project Server 2016 upgrade process](#): Get a high-level overview of how to upgrade from Project Server 2013 to Project Server 2016.
- [Plan to upgrade to Project Server 2016](#): Look at planning considerations when upgrading from Project Server 2013 to Project Server 2016, including system requirements.
- [Upgrading to Project Server 2016](#): See the detailed instructions on the upgrade process.

Step 2: Migrate to Project Server Subscription Edition

After you move to Project Server 2016 and verify that your data has migrated successfully, the next step is to migrate to Project Server Subscription Edition.

For more information, see [Upgrade to Project Server Subscription Edition](#).

Key resources:

- [Overview of the Project Server Subscription Edition upgrade process](#): Understand what you need to do to upgrade from Project Server 2013 to Project Server 2016.
- [Plan for upgrade to Project Server Subscription Edition](#): Look at the planning considerations to make when upgrading from Project Server 2013 to Project Server 2016.
- [Upgrading to Project Server Subscription Edition](#): See the detailed instructions on the upgrade process.

Resources to help you upgrade from Office 2010 servers and clients

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

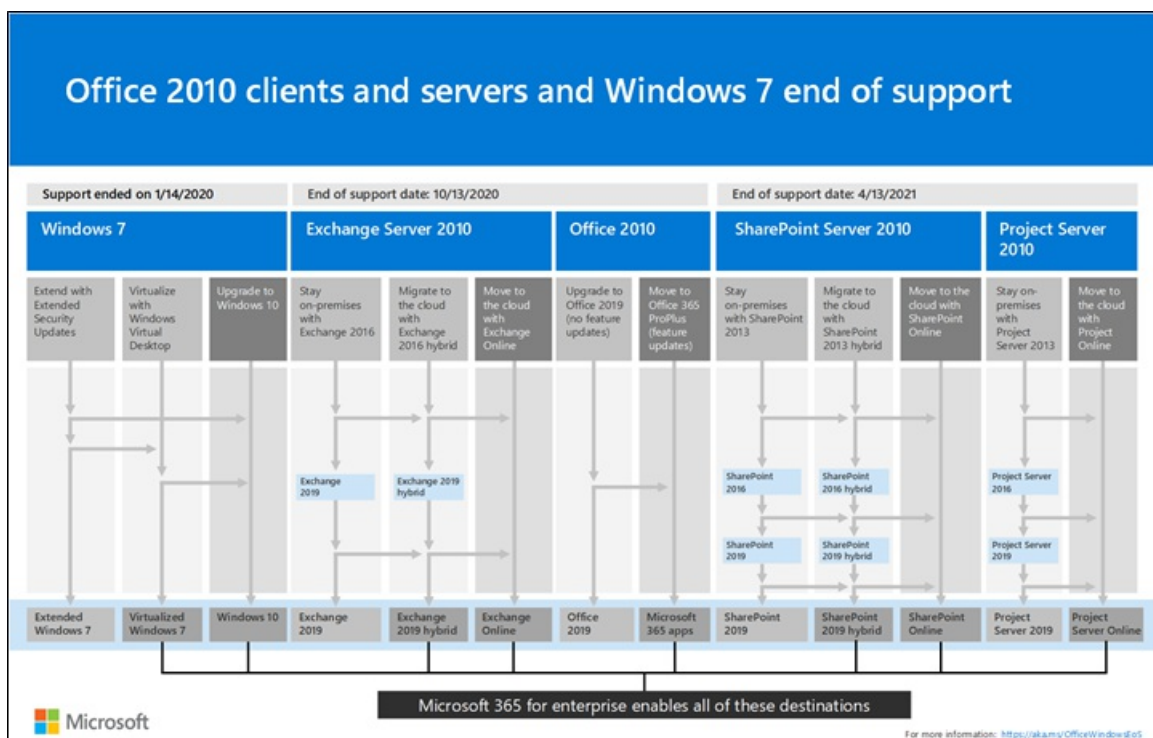
Office 2010 and Exchange 2010 reached their end of support on **October 13, 2020**.

SharePoint 2010 and Project Server 2010 will reach their end of support on **April 13, 2021**.

While you plan your upgrade, consider moving to Microsoft 365.

- Microsoft 365 has cloud-based services for Office 2010 server products, such as Exchange Server and SharePoint Server, and services, such as Teams and OneDrive for Business.
- Microsoft 365 Apps for enterprise (previously named *Office 365 ProPlus*), which is included with Microsoft 365 E3 and E5, is the set of Office client apps that you install on your local device. They're updated with new productivity and security features regularly from the Microsoft cloud.

For a visual summary of the upgrade, migration, and move-to-the-cloud options for Office 2010 clients and servers and Windows 7, see the [end of support poster](#).



This one-page poster summarizes the various paths you can take to handle Office 2010 client and server products and Windows 7 from reaching end of support. Preferred paths and option support in Microsoft 365 Enterprise are highlighted.

You can also [download](#) this poster and print it in letter, legal, or tabloid (11 x 17) format.

Office 2010 client and server upgrade planning

FOR THIS PRODUCT	WITH THIS END OF SUPPORT DATE	SEE THIS RESOURCE
Office 2010 (including Word 2010, Excel 2010, PowerPoint 2010, and Outlook 2010)	October 13, 2020	Office 2010 end of support roadmap
Exchange Server 2010	October 13, 2020	Exchange 2010 end of support roadmap
SharePoint 2010 or SharePoint Server 2010	April 13, 2021	Upgrading from SharePoint 2010
Project Server 2010	April 13, 2021	Project Server 2010 end of support roadmap
Lync Server 2010	April 13, 2021	Plan to upgrade to Skype for Business Server

I'm a home user. What do I do?

If you use Office 2010 products and applications at home, see [this information](#).

Related topics

[Video: What is Microsoft 365?](#)

[Microsoft Lifecycle Policy](#)

[Plan your upgrade from Office 2007 or Office 2010 servers and clients](#)

Exchange 2010 end of support roadmap

10/28/2022 • 13 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Exchange Server 2010 reached its end of support on **October 13, 2020**. If you haven't already begun your migration from Exchange 2010 to Microsoft 365, Office 365, or Exchange 2016, now's the time to start planning.

What does *end of support* mean?

Most Microsoft products have a support lifecycle during which they get new features, bug fixes, security fixes, and so on. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. Because Exchange 2010 reached its end of support on October 13, 2020, Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

Your installation of Exchange 2010 will continue to run after this date. But because of the changes listed above, we strongly recommend that you migrate from Exchange 2010 as soon as possible.

For more information about nearing the end of support, see [Resources to help you upgrade from Office 2010 servers and clients](#).

What are my options?

It's a great time to explore your options and prepare a migration plan. You can:

- Migrate fully to Microsoft 365. Migrate mailboxes using cutover, minimal hybrid, or full hybrid migration. Then remove on-premises Exchange servers and Active Directory.
- Migrate your Exchange 2010 servers to Exchange 2016 on your on-premises servers.

IMPORTANT

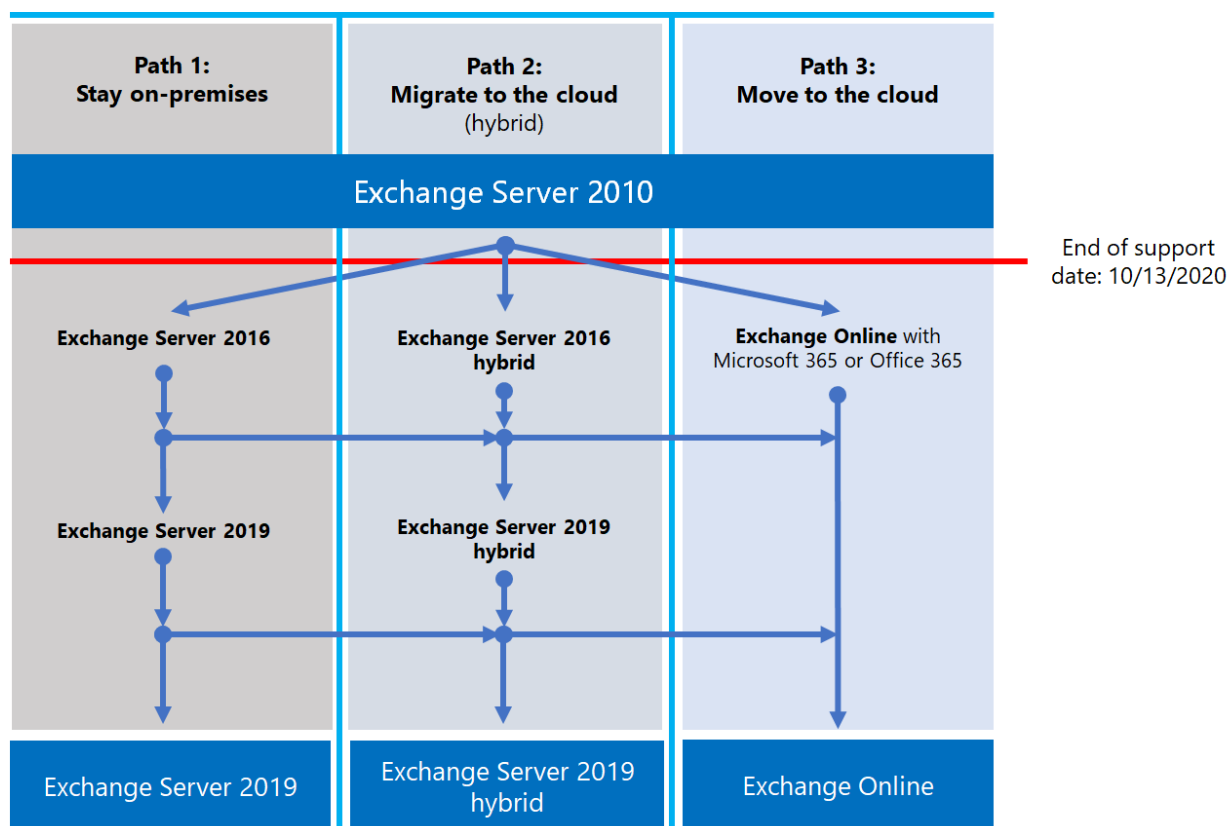
If your organization chooses to migrate mailboxes to Microsoft 365 but plans to keep DirSync or Azure AD Connect in place to continue managing user accounts from on-premises Active Directory, you need to keep at least one Microsoft Exchange server on-premises. If you remove all Exchange servers, you won't be able to make changes to Exchange recipients in Exchange Online because the source of authority remains in your on-premises Active Directory. Changes need to be made there. In this scenario, you have the following options:

- *Recommended:* If you migrated your mailboxes to Microsoft 365 and upgraded your servers by October 13, 2020, use Exchange 2010 to connect to Microsoft 365 and migrate mailboxes. Next, migrate Exchange 2010 to Exchange 2016, and decommission any remaining Exchange 2010 servers.
- If you didn't complete the mailbox migration and on-premises server upgrade by October 13, 2020, upgrade your on-premises Exchange 2010 servers to Exchange 2016 first. Then use Exchange 2016 to connect to Microsoft 365 and migrate mailboxes.

NOTE

It's little more complicated, but you can also migrate mailboxes to Microsoft 365 while migrating your on-premises Exchange 2010 servers to Exchange 2016.

Here are the three paths you can take to avoid the end of support for Exchange Server 2010.



The following sections explore each option in more detail.

Migrate to Microsoft 365

Migrating your email to Microsoft 365 is the best and simplest option to help you retire your Exchange 2010 deployment. With a migration to Microsoft 365, you can make a single hop from old technology to current features, including:

- Compliance capabilities such as Retention Policies, In-Place and Litigation Hold, in-place eDiscovery, and more.
- Microsoft Teams.
- Power BI.
- Focused Inbox.
- MyAnalytics.

Microsoft 365 also gets new features and experiences first, so your organization can start using them right away. Also, you won't have to worry about:

- Purchasing and maintaining hardware.
- Paying to heat and cool your servers.
- Keeping up to date on security, product, and time-zone fixes.
- Maintaining storage and software to support compliance requirements.
- Upgrading to a new version of Exchange. You're always on the latest version of Exchange in Microsoft 365.

How should I migrate to Microsoft 365?

Depending on your organization, you have a few options to get to Microsoft 365. First, you need to consider a few things, such as:

- The number of seats or mailboxes you need to move.
- How long you want the migration to last.
- Whether you need a seamless integration between your on-premises installation and Microsoft 365 during the migration.

This table shows your migration options and the most important factors that determine which method to use.

MIGRATION OPTION	ORGANIZATION SIZE	DURATION
Cutover migration	Fewer than 150 seats	A week or less
Minimal hybrid migration	Fewer than 150 seats	A few weeks or less
Full hybrid migration	More than 150 seats	A few weeks or more

The following sections give you an overview of these methods. For more information, see [Decide on a migration path](#).

Cutover migration

In a cutover migration, you migrate all your mailboxes, distribution groups, contacts, and so on, to Office 365 at a set date and time. When you're done, you shut down your on-premises Exchange servers and start using Microsoft 365 exclusively.

Cutover migration is great for small organizations that don't have many mailboxes, want to get to Microsoft 365 quickly, and don't want to deal with the complexity of the other methods. But it should be completed in a week or less. And it requires users to reconfigure their Outlook profiles. Cutover migration can migrate up to 2,000 mailboxes, but we recommend you use it for a maximum of 150. If you try to migrate more, you could run out of time to transfer all the mailboxes before your deadline, and your IT support staff may get overwhelmed with requests to help users reconfigure Outlook.

Here are things to consider about cutover migration:

- Microsoft 365 will need to connect to your Exchange 2010 servers by using Outlook Anywhere over TCP port 443.
- All on-premises mailboxes will be moved to Microsoft 365.
- You'll need an on-premises administrator account that has read access to your users' mailboxes.
- The Exchange 2010 accepted domains that you want to use in Microsoft 365 need to be added as verified domains in the service.
- Between when you start the migration and when you begin the completion phase, Microsoft 365 will periodically synchronize the Microsoft 365 and on-premises mailboxes. This lets you complete the migration without worrying about email being left behind in your on-premises mailboxes.
- Users will receive new temporary passwords for their Microsoft 365 account. They'll need to change those when they sign in to their mailboxes for the first time.
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users will need to set up a new Outlook profile on each of their devices and download their email again. The amount of email that Outlook will download can vary. For more information, see [Work offline in Outlook](#).

To learn more about cutover migration, see:

- [What you need to know about a cutover email migration](#)

- [Perform a cutover migration of email to Office 365](#)

Minimal hybrid migration

In a minimal hybrid, or express, migration you move a few hundred mailboxes to Microsoft 365 within a few weeks. This method doesn't support advanced hybrid-migration features like shared free/busy calendar information.

Minimal hybrid migration is great for organizations that need to take more time to migrate their mailboxes to Microsoft 365, but still plan to complete the migration within a few weeks. You get some of the benefits of the more advanced *full-hybrid migration* without much of the complexity. You can control how many and which mailboxes to migrate at a given time. Microsoft 365 mailboxes will be created with the user names and passwords of the on-premises accounts. And, unlike cutover migrations, your users don't have to recreate their Outlook profiles.

Here are things to consider about minimal hybrid migration:

- You'll need to do a one-time directory synchronization between your on-premises Active Directory servers and Microsoft 365.
- Users will be able to sign in to their Microsoft 365 mailbox with the same user name and password as before their mailbox.
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox that you migrate.
- Users won't need to set up a new Outlook profile on most of their devices, though some older Android phones might need a new profile. Users won't need to redownload their email.

For more information, see [Use Minimal Hybrid to quickly migrate Exchange mailboxes to Office 365](#).

Full hybrid

In a full hybrid migration, you have many hundreds, up to tens of thousands, of mailboxes, and you move some or all to Microsoft 365. Because these migrations are typically longer-term, hybrid migrations make it possible to:

- Show on-premises users the free/busy calendar information for users in Microsoft 365, and vice versa.
- See a unified global address list that contains recipients in both on-premises and Microsoft 365.
- View full Outlook recipient properties for all users, regardless of whether they're on-premises or in Microsoft 365.
- Secure email communication between on-premises Exchange servers and Office 365 using TLS and certificates.
- Treat messages sent between on-premises Exchange servers and Microsoft 365 as internal, enabling them to:
 - Be properly evaluated and processed by transport and compliance agents targeting internal messages.
 - Bypass anti-spam filters.

Full hybrid migrations are best for organizations that expect to stay in a hybrid configuration for many months or more. You get the features listed earlier in this section, plus directory synchronization, better integrated compliance features, and the ability to move mailboxes to and from Microsoft 365 using online mailbox moves. Microsoft 365 becomes an extension of your on-premises organization.

Things to consider about full-hybrid migration:

- They aren't suited to all organizations. Due to the complexity of full hybrid migrations, organizations with less than a few hundred mailboxes don't typically see benefits that justify the effort and cost involved. In such cases, we recommend that you consider cutover or minimal hybrid migration instead.
- You need to set up directory synchronization using Azure Active Directory (Azure AD) Connect between your on-premises Active Directory servers and Microsoft 365.

- Users will be able to sign in to their Microsoft 365 mailbox with same user name and password they use when they sign in to the local network. (This functionality requires Azure AD Connect with password synchronization and/or Active Directory Federation Services).
- You need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users don't need to set up a new Outlook profile on most of their devices, although some older Android phones might need a new profile. Users won't need to redownload their email.

IMPORTANT

If your organization chooses to migrate mailboxes to Microsoft 365 but plans to keep DirSync or Azure AD Connect in place to continue managing user accounts from on-premises Active Directory, you need to keep at least one Exchange server on-premises. If all Exchange servers are removed, you won't be able to make changes to Exchange recipients in Exchange Online. This is because the source of authority remains in your on-premises Active Directory and changes need to be made there.

If a full hybrid migration sounds right for you, see the following helpful resources:

- [Exchange Deployment Assistant](#)
- [Exchange Server Hybrid Deployments](#)
- [Hybrid Configuration wizard](#)
- [Hybrid Configuration wizard FAQs](#)
- [Hybrid deployment prerequisites](#)

Upgrade to a newer version of Exchange Server on-premises

We strongly believe that you get the best value and user experience by migrating fully to Microsoft 365. But we understand that some organizations need to keep some Exchange Servers on-premises. This might be because of regulatory requirements, to guarantee data isn't stored in a foreign datacenter, because you have unique settings or requirements that can't be met in the cloud, or because you need Exchange to manage cloud mailboxes because you still use Active Directory on-premises. In any case, if you keep Exchange on-premises, you should ensure your Exchange 2010 environment is upgraded to at least Exchange 2013 or Exchange 2016.

For the best experience, we recommend that you upgrade your remaining on-premises environment to Exchange 2016. You don't need to install Exchange Server 2013 if you want to go straight from Exchange Server 2010 to Exchange Server 2016.

Exchange 2016 includes all the features of previous releases of Exchange. It most closely matches the experience available with Microsoft 365, although some features are available only in Microsoft 365. Check out just a few of the things you've been missing:

EXCHANGE RELEASE	FEATURES
Exchange 2013	Simplified architecture reduces the number of server roles to three (Mailbox, Client Access, Edge Transport)
	Data loss prevention policies (DLP) that help keep sensitive information from leaking
	Improved Outlook Web App experience
Exchange 2016	<i>Features from Exchange 2013 and ...</i>

EXCHANGE RELEASE	FEATURES
	Further simplified server roles to just Mailbox and Edge Transport
	Improved DLP along with integration with SharePoint
	Improved database resilience
	Online document collaboration
CONSIDERATION	MORE INFORMATION
End of support dates	Like Exchange 2010, each version of Exchange has its own end-of-support date: Exchange 2013 - April 2023 Exchange 2016 - October 2025 The earlier the end-of-support date, the sooner you'll need to perform another migration. April 2023 is a lot closer than you think!
Migration path to Exchange 2013 or 2016	The migration path from Exchange 2010 to a newer version is the same whether you choose Exchange 2013 or Exchange 2016: Install Exchange 2013 or 2016 into your existing Exchange 2010 organization. Move services and other infrastructure to Exchange 2013 or 2016. Move mailboxes and public folders to Exchange 2013 or 2016 Decommission remaining Exchange 2010 servers.
Version coexistence	When migrating to Exchange 2013 or Exchange 2016, you can install either version into an existing Exchange 2010 organization. This enables you to install one or more Exchange 2013 or Exchange 2016 servers and do your migration.
Server hardware	Server hardware requirements have changed from Exchange 2010. Make sure your hardware is compatible. Find out more about hardware requirements for each version here: Exchange 2016 system requirements Exchange 2013 system requirements With the significant improvements in Exchange performance and the increased computing power and storage capacity in newer servers, you'll likely need fewer servers to support the same number of mailboxes.

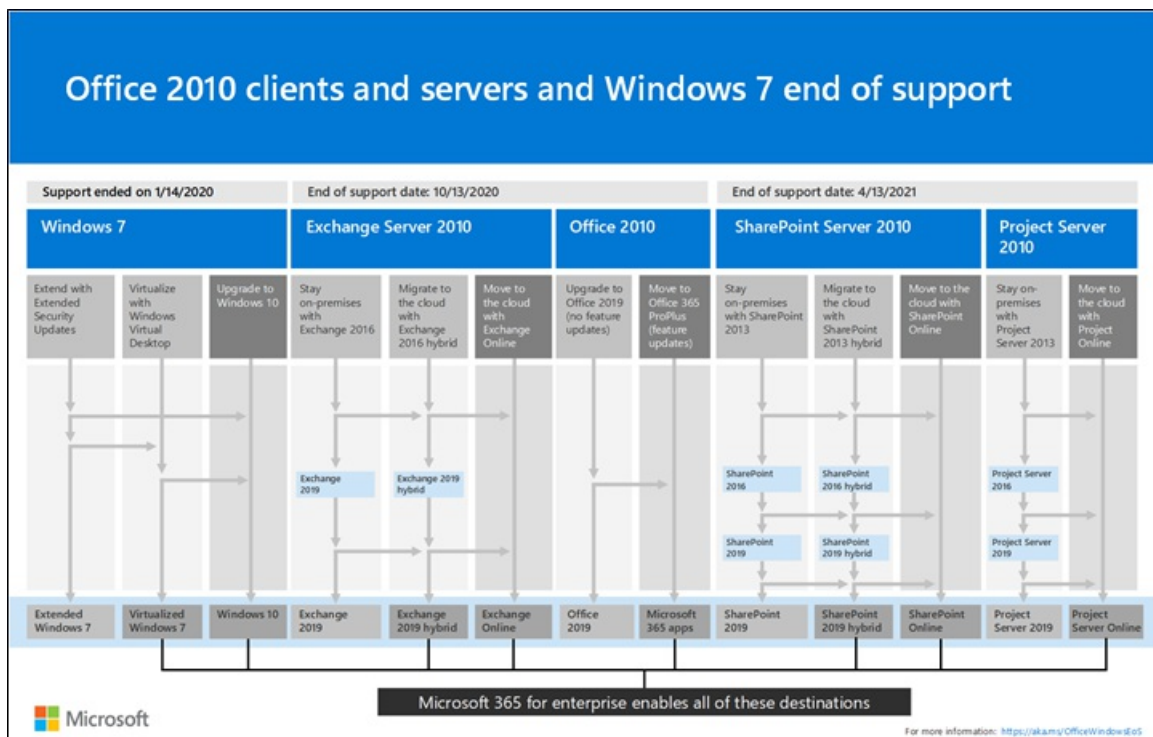
CONSIDERATION	MORE INFORMATION
Operating system version	The minimum supported operating system versions for each version are: Exchange 2016 - Windows Server 2012 Exchange 2013 - Windows Server 2008 R2 SP1 You can find more information about operating system support at Exchange Supportability Matrix.
Active Directory forest functional level	The minimum supported Active Directory forest functional levels for each version are: Exchange 2016 - Windows Server 2008 R2 SP1 Exchange 2013 - Windows Server 2003 You can find more information about forest functional level support at Exchange Supportability Matrix.
Office client versions	The minimum supported Office client versions for each version are: Exchange 2016 - Office 2010 (with the latest updates) Exchange 2013 - Office 2007 SP3 Find more information about Office client support at Exchange Supportability Matrix.

Use the following resources to help with your migration:

- [Exchange Deployment Assistant](#)
- Active Directory schema changes for Exchange [2016](#), [2013](#)
- System requirements for Exchange [2016](#), [2013](#)
- Prerequisites for Exchange [2016](#), [2013](#)

Summary of options for Office 2010 client and servers and Windows 7

For a visual summary of the upgrade, migrate, and move-to-the-cloud options for Office 2010 clients and servers and Windows 7, see the [end of support poster](#).



This one-page poster illustrates the various paths you can take to respond to Office 2010 client and server products and Windows 7 reaching end of support, with preferred paths and option support in Microsoft 365 Enterprise highlighted.

You can also [download](#) this poster and print it in letter, legal, or tabloid (11 x 17) format.

What if I need help?

If you're migrating to Microsoft 365, you might be eligible to use our Microsoft FastTrack service. FastTrack provides best practices, tools, and resources to make your migration to Microsoft 365 as seamless as possible. Best of all, you'll have a support engineer walk you through from planning and design to migrating your last mailbox. For more about FastTrack, see [Microsoft FastTrack](#).

If you run into problems during your migration to Microsoft 365 and you aren't using FastTrack, or you're migrating to a newer version of Exchange Server, here are some resources you can use:

- [Technical community](#)
- [Customer support](#)

Related articles

[Resources to help you upgrade from Office 2010 servers and clients](#)

Upgrading from SharePoint 2010

10/28/2022 • 14 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft SharePoint 2010 and SharePoint Server 2010 will reach end of support on **April 13, 2021**. This article provides resources to help you migrate your existing SharePoint Server 2010 data to SharePoint Online in Microsoft 365 or upgrade your on-premises SharePoint Server 2010 environment.

What is *end of support*?

Most Microsoft products have a support lifecycle, during which they get new features, bug fixes, security fixes, and so on. After the end-of-support date, the product doesn't stop working, but Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

That means there will be no further updates, patches, or fixes for the product (including security patches/fixes). Microsoft Support will have fully shifted its support efforts to more recent versions.

As the end of support of SharePoint Server 2010 approaches, delete data you no longer need before you upgrade the product and migrate your important data.

NOTE

A software lifecycle typically lasts for ten years from the initial release. [Microsoft solution providers](#) can help you upgrade to the next version of the software or migrate to Microsoft 365 migration (or both). Make sure you're aware of end-of-support dates for critical underlying technologies as well, particularly for the version of Microsoft SQL Server you're using with SharePoint. For more information, see [Fixed Lifecycle Policy](#).

Plan ahead

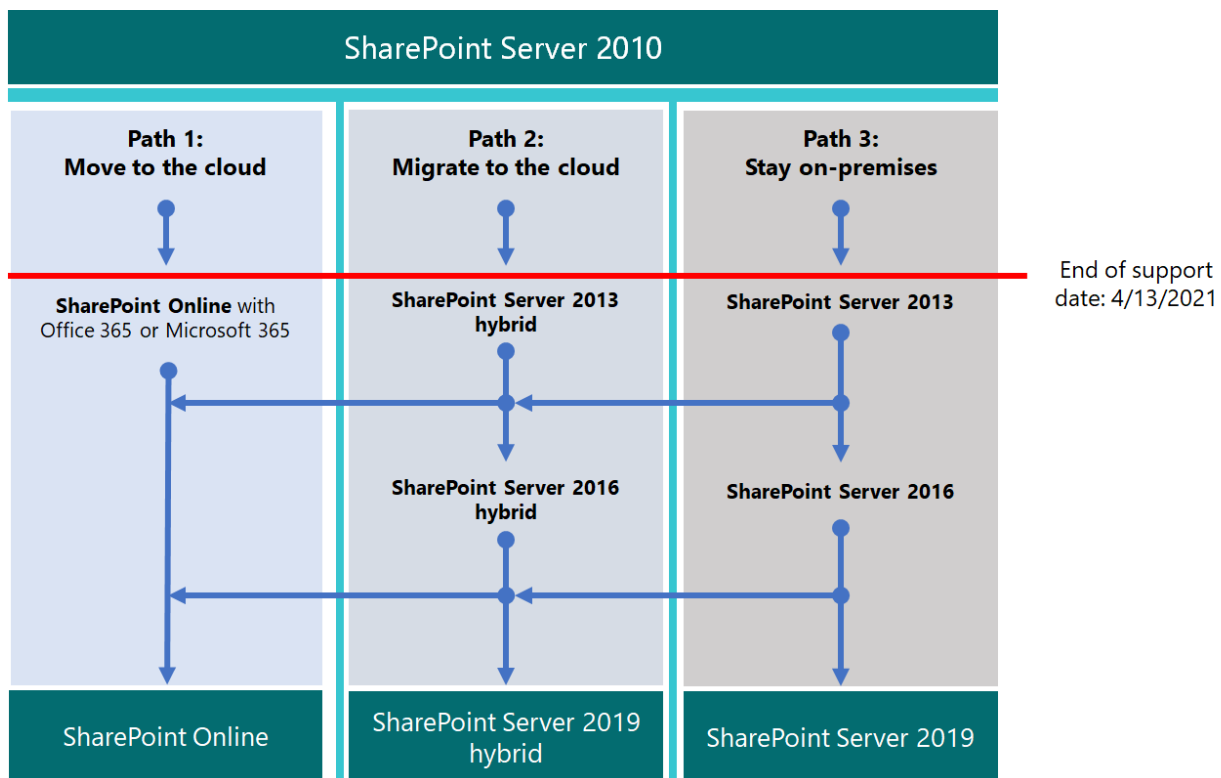
Check the dates that support ends on the [Product Lifecycle site](#). Plan your upgrades or migrations with these dates in mind. Remember that your product *won't stop working* at the date listed. But because your installation will no longer be patched after that date, you'll want to plan a smooth transition to the next version of the product.

This matrix helps plot a course among migration options:

END OF SUPPORT PRODUCT	GOOD	BEST
SharePoint Server 2010	SharePoint Server 2013 (on-premises)	SharePoint Online
	SharePoint Server 2013 hybrid with SharePoint Online	SharePoint Server 2016 (on-premises)
		SharePoint Cloud Hybrid Search

If you choose an option on the low end of the scale (good), you'll need to start planning for another upgrade soon after your migration from SharePoint Server 2010.

Here are the three paths you can take to avoid the end of support for SharePoint Server 2010.



NOTE

End of support for SharePoint Server 2010 and SharePoint Foundation 2010 is currently scheduled for April 13, 2021. But make sure to check the [Product Lifecycle site](#) for the most-current dates.

What's next?

SharePoint Server 2013 and SharePoint Foundation 2013 can be installed on-premises on your own servers. Or you can use SharePoint Online, which is an online service that's part of Microsoft 365. You can choose to:

- Migrate to SharePoint Online.
- Upgrade SharePoint Server or SharePoint Foundation on-premises.
- Do both of the above.
- Implement a [SharePoint hybrid](#) solution.

Consider the hidden costs of maintaining a server farm, including maintaining or migrating customizations and upgrading hardware. If you've accounted for these factors, it will be easier to upgrade on-premises. If you run your farm on legacy SharePoint Servers without heavy customization, you could benefit from a planned migration to SharePoint Online. For an on-premises SharePoint Server environment, you can also consider moving some data in SharePoint Online to reduce hardware management overhead.

NOTE

SharePoint administrators can create a Microsoft 365 Subscription, set up new SharePoint Online sites, and then cut away from SharePoint Server 2010 cleanly, taking only essential documents to the fresh sites. Then, any remaining data can be drained from the SharePoint Server 2010 site into on-premises archives.

SHAREPOINT ONLINE	SHAREPOINT SERVER ON-PREMISES
High cost in time (plan/execution/verification)	High cost in time (plan/execution/verification)
Lower cost in funds (no hardware purchases)	Higher cost in funds (hardware purchases)
One-time cost in migration	One-time cost repeated per future migration
Low total cost of ownership/maintenance	High total cost of ownership/maintenance

A one-time move to Microsoft 365 will have a higher cost while you organize data and decide what to take to the cloud and what to leave behind. But after your data is migrated, future upgrades will be automatic, as you'll no longer need to manage hardware and software updates. And the up time of your farm will be backed by a [Microsoft service level agreement \(SLA\)](#).

Migrate to SharePoint Online

Make sure SharePoint Online offers all the features you need. See [SharePoint service description](#).

You can't migrate directly from SharePoint Server 2010 (or SharePoint Foundation 2010) to SharePoint Online. So much of the migration work is manual. But this stage gives you the opportunity to prune data and sites that are no longer needed before the move. You can archive other data into storage.

Remember that SharePoint Server 2010 and SharePoint Foundation 2010 won't stop working at end of support. So administrators can have a period when SharePoint is still running if their customers forget to move some of their data.

If you upgrade to SharePoint Server 2013 or SharePoint Server 2016 and decide to put data into SharePoint Online, you might use the [SharePoint Migration API](#) to migrate information into OneDrive for Business.

SHAREPOINT ONLINE ADVANTAGE	SHAREPOINT ONLINE DISADVANTAGE
Microsoft supplies SPO hardware and all hardware administration.	Available features may differ between SharePoint Server on-premises and SPO.
You're the SharePoint admin or global admin of your subscription and can assign administrators to SPO sites.	Some actions available to a farm administrator in SharePoint Server on-premises don't exist (or aren't necessary) in the SharePoint Administrator role in Microsoft 365. But SharePoint Administration, Site Collection Administration, and Site Ownership are local to your org.
Microsoft applies patches, fixes, and updates to underlying hardware and software, including SQL servers on which SharePoint Online runs.	Because there's no access to the underlying file system in the service, customization is limited.
Microsoft publishes service level agreements and moves quickly to resolve service-level incidents.	Backup and restore and other recovery options are automated by the service in SharePoint Online. Backups are overwritten if not used.
Security testing and server performance tuning are carried out continuously in the service by Microsoft.	Changes to the user interface and other SharePoint features are installed by the service and may need to be toggled on or off.
Microsoft 365 meets many industry standards: Microsoft compliance offerings .	FastTrack assistance for migration is limited. Much of the upgrade will be manual or via the SPO Migration API described in the SharePoint Online and OneDrive Migration Content Roadmap .

SHAREPOINT ONLINE ADVANTAGE	SHAREPOINT ONLINE DISADVANTAGE
Microsoft Support engineers and datacenter employees don't have unrestricted admin access to your subscription.	There can be additional costs if hardware infrastructure needs to be upgraded to support the newer version of SharePoint or if a secondary farm is required for upgrade.
Solution providers can help with the one-time job of migrating your data to SharePoint Online.	Not all changes to SharePoint Online are within your control. After migration, design differences in menus, libraries, and other features may temporarily affect usability.
Online products are updated automatically across the service. Features may deprecate, but there's no true end of support lifecycle.	There's an end-of-support lifecycle for SharePoint Server or SharePoint Foundation as well as underlying SQL servers.

If you've decided to create a new Microsoft 365 site and will manually migrate data to it as is needed, check your [Microsoft 365 options](#).

Upgrade SharePoint Server on-premises

As of SharePoint Server 2019, upgrades must go *serially*. There's no way to upgrade from SharePoint Server 2010 to SharePoint Server 2016 or to SharePoint 2019 directly. Serial upgrade path:

- SharePoint Server 2010 > SharePoint Server 2013 > SharePoint Server 2016

It will take time and planning to follow the entire path from SharePoint 2010 to SharePoint Server 2016. Upgrades involve costs for hardware (SQL servers must also be upgraded), software, and administration. Also, customizations may need to be upgraded or even abandoned. Be sure that you document critical customizations before you upgrade your SharePoint Server farm.

NOTE

It's possible to maintain your end-of-support SharePoint 2010 farm, install a SharePoint Server 2016 farm on new hardware (so the separate farms run side-by-side), and then plan and execute a manual migration of content (for downloading and re-uploading content, for example). But there are potential pitfalls to these manual moves, such as documents coming from 2010 having a current last-modified account with the alias of the account that does the manual move. And some work must be done ahead of time, such as recreating sites, subsites, permissions, and list structures. Be sure to clean your environment prior to upgrade. Consider what data you can move into storage or no longer need. This can reduce the impact of migration. Be certain your existing farm is functional before you upgrade, and (certainly) before you decommission!

Remember to review the *supported and unsupported upgrade paths*:

- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

If you have *customizations*, it's critical that you plan for each step in the migration path:

- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

ON-PREMISES ADVANTAGE	ON-PREMISES DISADVANTAGE
Full control of all aspects of your SharePoint Farm (and its SQL), from the server hardware up.	All breaks and fixes are the responsibility of your company. But you can engage paid Microsoft Support if your product isn't past end of support.

ON-PREMISES ADVANTAGE	ON-PREMISES DISADVANTAGE
Full feature set of SharePoint Server on-premises with the option to connect your on-premises farm to a SharePoint Online subscription via hybrid.	Upgrade, patches, security fixes, hardware upgrades, and all maintenance of SharePoint Server and its SQL farm are managed on-premises.
Full access for greater customization options than with SharePoint Online.	Microsoft compliance offerings must be manually configured on-premises.
Security testing and server performance tuning are carried out on your premises under your control.	Microsoft 365 may make features available to SharePoint Online that don't interoperate with SharePoint Server on-premise.
Solution providers can help migrate data to the next version of SharePoint Server (and beyond).	Your SharePoint Server sites will not automatically use SSL/TLS certificates as is seen in SharePoint Online.
Full control of naming conventions and backup and restore and other recovery options in SharePoint Server on-premises.	SharePoint Server on-premises is sensitive to product lifecycles.

Upgrade resources

Begin by comparing hardware and software requirements. If your current environment doesn't meet basic requirements, you may have to upgrade the hardware in the farm or the SQL servers first.

You may decide to move some of your sites to the "evergreen" hardware of SharePoint Online. Once you've made your assessment, follow supported upgrade paths and methods.

- *Hardware/software requirements for:*

[SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- *Software boundaries and limits for:*

[SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- *The upgrade process overview for:*

[SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

Create a hybrid solution with SharePoint Online and SharePoint Server on-premises

A hybrid setup provides the best of both on-premises and online for some migration needs. You can connect SharePoint Server 2013, 2016, or 2019 farms to SharePoint Online to create a SharePoint hybrid: [Learn about SharePoint hybrid solutions](#).

If a hybrid SharePoint Server farm is your migration goal, figure what sites and users to move online and which need to remain on-premises. Ranking your SharePoint Server farm content as high, medium, or low impact to your company can help with this decision. You may only need to share user accounts for login and the SharePoint Server search index with SharePoint Online. But this factor may not be clear until you look at how your sites are used. If your company later decides to migrate all your content to SharePoint Online, you can move all remaining accounts and data online and decommission your on-premises farm. Management/administration of the SharePoint farm will be done through Microsoft 365 consoles from that point on.

Be sure to familiarize yourself with the existing types of hybrids and how to configure the connection between your on-premises SharePoint farm and your Microsoft 365 subscription.

OPTION	DESCRIPTION
Microsoft compliance offerings.	FastTrack assistance for migration is limited. Much of the upgrade will be manual or via the SPO Migration API described in the SharePoint Online and OneDrive Migration Content Roadmap.
Microsoft Support engineers and datacenter employees don't have unrestricted admin access to your subscription.	There may be additional costs if hardware infrastructure needs to be upgraded to support the newer version of SharePoint, or if a secondary farm is required.
Partners can assist with the one-time job of migrating your data to SharePoint Online.	
Online products are updated automatically across the service. Features may deprecate, but there's no true end of support.	

If you've decided to create a new Microsoft 365 site and manually migrate data to it as is needed, check your [Microsoft 365 options](#).

Upgrade SharePoint Server on-premises

There's no way to skip versions in SharePoint Upgrades. That means upgrades go serially:

- SharePoint 2007 > SharePoint Server 2010 > SharePoint Server 2013 > SharePoint Server 2016

To take the entire path from SharePoint 2007 to SharePoint Server 2016 will mean a significant investment of time and will involve hardware (SQL servers must also be upgraded), software, and administration costs. Customizations will need to be upgraded or abandoned, according to the criticality of the feature.

NOTE

It's possible to maintain your end-of-life SharePoint 2007 farm, install a SharePoint Server 2016 farm on new hardware (so the separate farms run side-by-side), and then plan and execute a manual migration of content (for downloading and re-uploading content, for example). But there are some drawbacks to these manual moves, such as moves of documents replacing the last modified account with the alias of the account that does the manual move. And much work must be done ahead of time, such as recreating sites, subsites, permissions, and list structures. In any case, consider what data you can move into storage or no longer need to reduce the impact of migration.

Make sure to clean your environment prior to upgrade. Be certain your existing farm is functional before you upgrade, and certainly before you decommission!

Remember to review the *supported and unsupported upgrade paths*:

- [SharePoint Server 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

If you have *customizations*, it's critical to plan your upgrade for each step in the migration path:

- [SharePoint 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

ON-PREMISES PRO	ON-PREMISES CON
Full control of all aspects of your SharePoint Farm, from the server hardware up.	All breaks and fixes are the responsibility of your company. (But you can engage paid Microsoft Support if your product isn't past end of support.)
Full feature set of SharePoint Server on-premises with the option to connect your on-premises farm to a SharePoint Online subscription via hybrid.	Upgrade, patches, security fixes, and all maintenance of SharePoint Server managed on-premises.
Full access for greater customization.	Microsoft compliance offerings must be manually configured on-premises.
Security testing and server performance tuning is carried out on your premises under your control.	Microsoft 365 may make features available to SharePoint Online that don't interoperate with SharePoint Server on-premises.
Partners can help migrate data to the next version of SharePoint Server (and beyond).	Your SharePoint Server sites will not automatically use SSL/TLS certificates as is seen in SharePoint Online.
Full control of naming conventions and backup and restore and other recovery options in SharePoint Server on-premises.	SharePoint Server on-premises is sensitive to product lifecycles.

Upgrade resources

Begin by knowing that you meet hardware and software requirements, then follow supported upgrade methods.

- *Hardware/software requirements for:*

[SharePoint Server 2010](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- *Software boundaries and limits for:*

[SharePoint Server 2007](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- *The upgrade process overview for:*

[SharePoint Server 2007](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

Create a SharePoint hybrid solution between SharePoint Online and on-premises

If the answer to your migration needs is somewhere between the control offered by on-premises and the lower cost of ownership offered by SharePoint Online, you can connect SharePoint Server 2013 or 2016 farms to SharePoint Online through hybrids. [Learn about SharePoint hybrid solutions](#)

If you decide that a hybrid SharePoint Server farm will benefit your business, familiarize yourself with the existing types of hybrids and how to configure the connection between your on-premises SharePoint farm and your Microsoft 365 subscription.

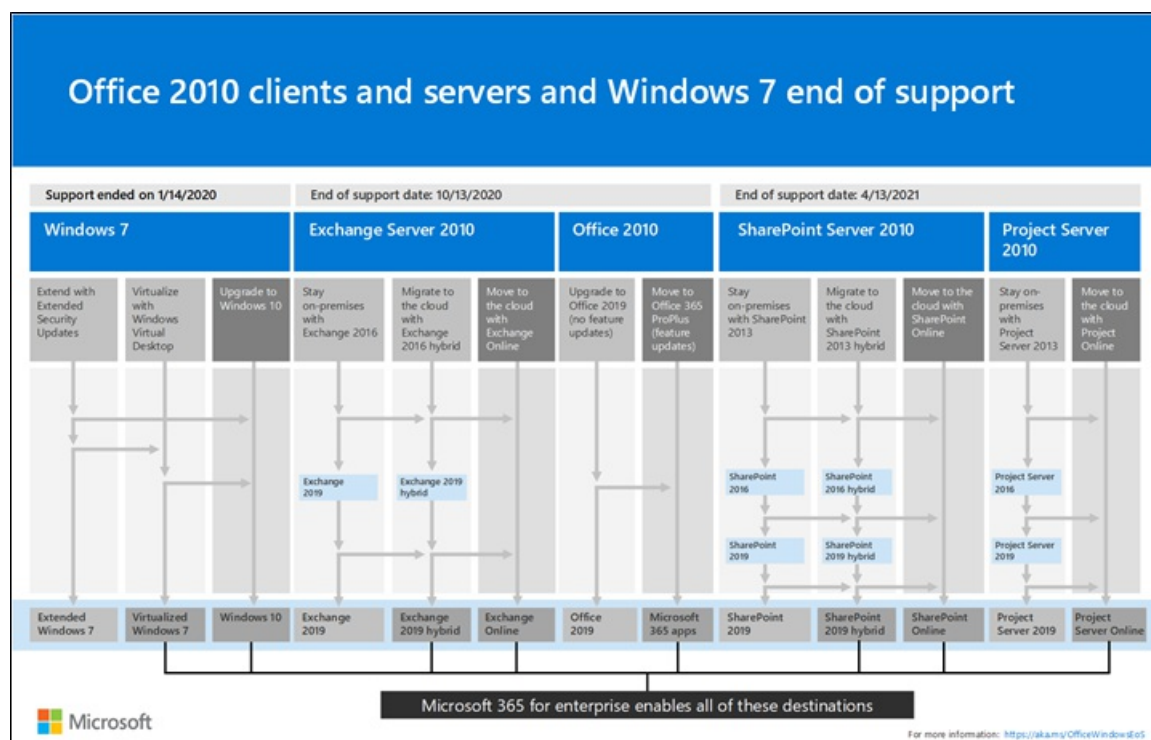
You may want to create a Microsoft 365 dev/test environment, which you can set up with [Test Lab Guides](#). After you get a trial or purchased Microsoft 365 subscription, you can create the site collections, webs, and document libraries in SharePoint Online to which you can migrate data. You can migrate manually, by use of the Migration API, or, if you want to migrate My Site content to OneDrive for Business, through the hybrid wizard.

NOTE

To use the hybrid option, your SharePoint Server 2010 farm must first be upgraded on-premises to SharePoint Server 2013 or 2016. SharePoint Foundation 2010 and SharePoint Foundation 2013 don't support hybrid connections with SharePoint Online.

Summary of options for Office 2010 client and servers and Windows 7

For a visual summary of the upgrade, migrate, and move-to-the-cloud options for Office 2010 clients and servers and Windows 7, see the [end of support poster](#).



This poster illustrates the various paths you can take to avoid Office 2010 client and server products and Windows 7 end of support, with preferred paths and option supports in Microsoft 365 Enterprise highlighted.

You can also [download](#) this poster and print it in letter, legal, or tabloid (11 x 17) format.

Related articles

[Resources to help you upgrade from Office 2007 or 2010 servers and clients](#)

[Overview of the upgrade process from SharePoint 2010 to SharePoint 2013](#)

[Best practices for upgrading from SharePoint 2010 to SharePoint 2013](#)

[Troubleshoot database upgrade issues in SharePoint 2013](#)

[Search for Microsoft solution providers to help with your upgrade](#)

[Updated Product Servicing Policy for SharePoint 2013](#)

[Updated Product Servicing Policy for SharePoint Server 2016](#)

Project Server 2010 end of support roadmap

10/28/2022 • 10 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Project Server 2010 will reach end of support on **April 13, 2021**. This date was extended from the previous end-of-support date of October 13, 2020. If you're currently using Project Server 2010, note that these related products have the following end-of-support dates:

PRODUCT	END OF SUPPORT DATE
Project 2010 Standard	October 13, 2020
Project 2010 Professional	October 13, 2020

For more information about reaching end of support, see [Upgrade from Office 2010 servers and client products](#).

What does *end of support* mean?

Almost all Microsoft products have a support lifecycle, during which they get new features, bug fixes, and security updates. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. After Project Server 2010 reaches its end of support on April 13, 2021, Microsoft will no longer provide:

- Technical support for problems that may occur.
- Bug fixes for issues that are discovered and that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that are discovered and that may make the server vulnerable to security breaches.
- Time zone updates.

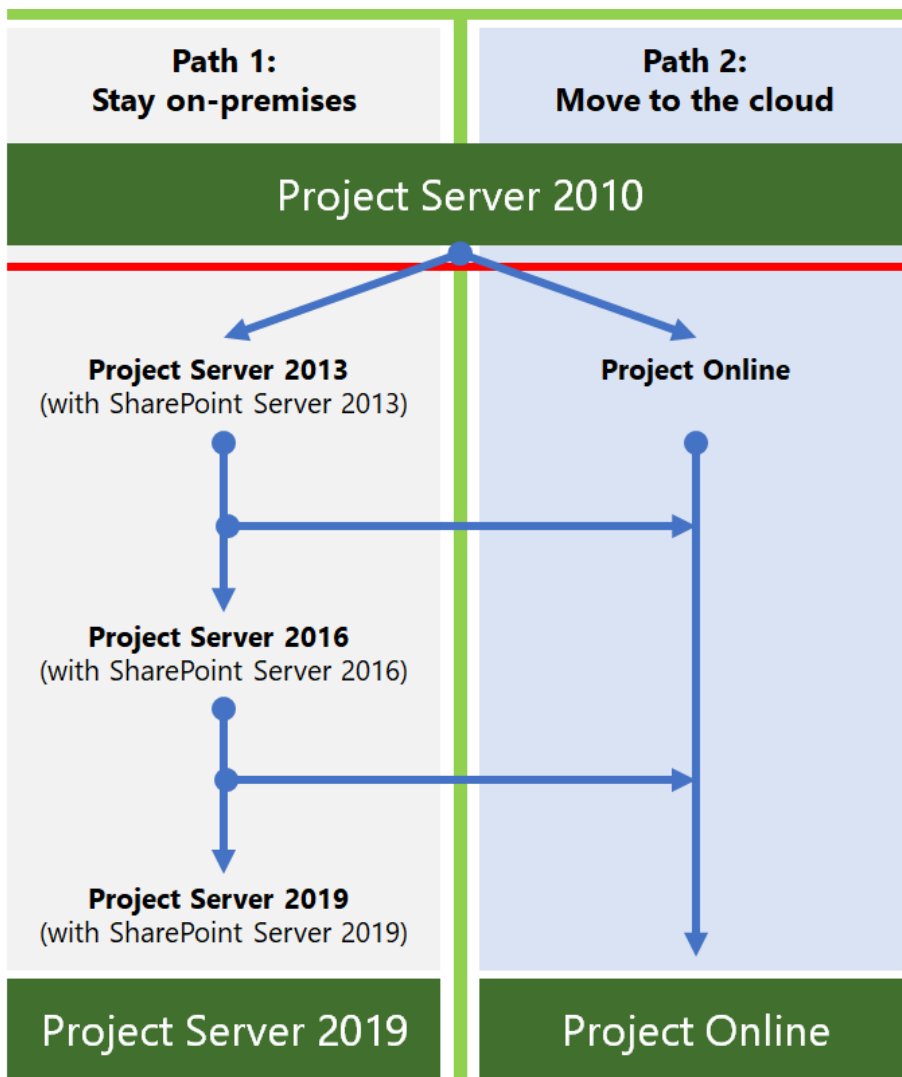
Your installation of Project Server 2010 will continue to run after this date. But, because of the changes listed previously, we strongly recommend that you migrate from Project Server 2010 as soon as possible.

What are my options?

Your migration options are:

- Migrate to Project Online
- Migrate to a newer on-premises version of Project Server (preferably Project Server 2019)

Here are the two paths you can take to avoid the end of support for Project Server 2010.



End of support
date: 4/13/2021

WHY WOULD I PREFER TO MIGRATE TO PROJECT SERVER 2019?	WHY WOULD I PREFER TO MIGRATE TO PROJECT ONLINE?
Business rules restrict me from operating my business in the cloud. I need control of updates to my environment.	I have mobile or remote users. Costs to migrate on-premises servers are a significant concern (hardware, software, time and effort to implement, and so on.). After migration, costs to maintain my environment are a concern (for example, automatic updates, guaranteed uptime, and so on.).

NOTE

For more information about your migration options, see [Resources to help you upgrade from Office 2010 servers and clients](#). Note that Project Server doesn't support hybrid configuration because Project Server and Project Online can't share the same resource pool.

What are my options for Project client?

If you're using Project Professional 2010 or Project Standard 2010, your options are:

- Move to a newer version of Project Professional or Project Standard
- Move to an online solution, such as Project Online or Project for the web

Move to a newer version of Project client

If you're migrating from Project Standard 2010, you can move to a newer version of Project Standard (Project Standard 2016 or Project Standard 2019). We recommend you move to the newest version to take advantage of the latest features. Migrating to a less-current version (Project Standard 2016) also means you'll need to migrate again sooner.

Similarly, if you're migrating from Project Professional 2010, you can move to a newer version (Project Professional 2019 or Project Professional 2016). Again, move to the newest version if possible. If you use Project Professional to connect to Project Server, make sure you migrate to a version of Project Professional that connects with the version of Project Server that you use.

Project Professional 2010 users can also migrate to the Project Online Desktop client, which is a subscription-based version of Project Professional 2019. It's included in Project Plan 3 and Project Plan 5 subscriptions.

Move to an online solution

You can also migrate from Project Professional 2010 or Project Standard 2010 to a Project subscription-based online solution. Both Project Plan 3 and Plan 5 include Project Online and the latest cloud offering, [Project for the web](#). Both offer new features and benefits that are worth exploring.

For more information about features and licenses, see [Microsoft Project service description](#).

Important considerations for migrating from Project Server 2010

Consider the following when you plan to migrate from Project Server 2010:

- **Get help from a Microsoft solution provider** - An upgrade from Project Server 2010 can be a challenge. It requires much preparation and planning. It can be especially challenging if you weren't the person who originally set up Project Server 2010. Microsoft solution providers are available to help, whether you plan to migrate to Project Server 2019 or to Project Online. Search for a solution provider in the [Microsoft solution provider center](#).
- **Plan for your customizations** - Customizations in your Project Server 2010 environment might not work when you migrate to Project Server 2019 or Project Online. There are significant differences in Project Server architecture between versions. Also, the required operating systems, database servers, and web browsers that work with the versions differ. Have a plan on how to test or rebuild your customizations in the new environment. Take this opportunity to determine if specific customizations are still needed. For more information, see [Create a plan for current customizations during upgrade to SharePoint 2013](#).
- **Time and patience** - Upgrade planning, execution, and testing will take considerable time and effort, especially for an upgrade to Project Server 2019. If you're migrating from Project Server 2010 to Project Server 2019, you must first migrate to Project Server 2013, check your data, then migrate to Project Server 2016, and then to Project Server 2019. You might want to check with a Microsoft solution provider for a time frame and estimated cost for them to assist.

Migrate to Project Online

If you choose to migrate from Project Server 2010 to Project Online, you can follow these steps to manually migrate your project plan data:

1. Save your project plans from Project Server 2010 to .mpp format.
2. Using Project Professional 2016, Project Professional 2019, or the Project Online Desktop Client, open each .mpp file, and then save and publish it to Project Online.

You can manually create your PWA configuration in Project Online (for example, recreate any needed custom fields or enterprise calendars). Microsoft solution providers can also help with this process.

Key resources:

RESOURCE	DESCRIPTION
Get started with Project Online	How to set up and use Project Online
Project Online Service Description	Information about the different Project Online plans available

Migrate to a newer on-premises version of Project Server

We strongly believe that you get the best value and user experience by migrating to Project Online. But we also understand some organizations need to keep project data on-premises. If you choose to keep your project data on-premises, you can migrate your Project Server 2010 environment to Project Server 2013, Project Server 2016, or Project Server 2019.

If you can't migrate to Project Online, we recommend that you migrate to Project Server 2019. Project Server 2019 includes most of the key features in previous releases of Project Server. And it most closely matches the experience available with Project Online, although some features are available only in Project Online.

After you complete each migration, make sure that your data migrated successfully.

NOTE

If you're limited to an on-premises solution and considering only migrating to Project Server 2013, beware that this version only has a few more years of support left. The end of support date for Project Server 2013 with Service Pack 2 is October 13, 2023. For more information about end-of-support dates, see [Microsoft Product Lifecycle Policy](#).

How do I migrate to Project Server 2019?

The architectural differences between Project Server 2010 and Project Server 2019 prevent a direct migration path. So you'll need to migrate your Project Server 2010 data to each successive version of Project Server until you reach Project Server 2019. Steps to upgrade Project Server 2010 to Project Server 2019:

1. Migrate to Project Server 2013.
2. Migrate from Project Server 2013 to Project Server 2016.
3. Migrate from Project Server 2016 to Project Server 2019.

After you complete each migration, make sure that your data migrated successfully.

Step 1: Migrate to Project Server 2013

For a comprehensive information about upgrading from Project Server 2010 to Project Server 2013, see [Upgrade to Project Server 2013](#).

Key resources:

- [Overview of the Project Server 2013 upgrade process](#)

Get a high-level overview of how to upgrade from Project Server 2010 to Project Server 2013.

- [Plan to upgrade to Project Server 2013](#)

Look at planning considerations when upgrading from Project Server 2010 to Project Server 2013, including system requirements.

- [What's new in Project Server 2013 upgrade](#) covers important changes for this version, including:

- There's no in-place upgrade to Project Server 2013. The database-attach method is the only supported way to upgrade from Project Server 2010 to Project Server 2013.
- The upgrade process will not only convert your Project Server 2010 data to Project Server 2013 format but will also consolidate the four Project Server 2010 databases into a single Project Web App database.
- Both SharePoint Server 2013 and Project Server 2013 changed to claims-based authentication from the previous version. If you're using classic authentication, you'll need to consider this when you upgrade. For more information, see [Migrate from classic-mode to claims-based authentication in SharePoint 2013](#).

Key resources:

- [Overview of the upgrade process to Project Server 2013](#)
- [Upgrade your databases and Project Web App site collections \(Project Server 2013\)](#)
- [Microsoft Project Server upgrade process diagram](#)
- [The Great Database Consolidation, Project Server 2010 to 2013 Migration in 8 Easy Steps](#)

Step 2: Migrate to Project Server 2016

After you move to Project Server 2013 and verify that your data has migrated successfully, the next step is to migrate to Project Server 2016.

For more information, see [Upgrade to Project Server 2016](#).

Key resources:

- [Overview of the Project Server 2016 upgrade process](#)

Understand what you need to do to upgrade from Project Server 2013 to Project Server 2016.

- [Plan for upgrade to Project Server 2016](#)

Look at the planning considerations to make when upgrading from Project Server 2013 to Project Server 2016.

[Things you need to know about Project Server 2016 upgrade](#) covers important changes for upgrading to this version, which include:

- When you create your Project Server 2016 environment, note that the Project Server 2016 installation files are included in SharePoint Server 2016. For more information, see [Deploy Project Server 2016](#).
- Resource plans are deprecated in Project Server 2016. Your Project Server 2013 resource plans will be migrated to Resource Engagements in Project Server 2016 and in Project Online. See [Overview: Resource engagements](#) for more information.

Step 3: Migrate to Project Server 2019

After you migrate to Project Server 2016 and verify that your data migrated successfully, the next step is to migrate your data to Project Server 2019.

To learn what you need to do to upgrade from Project Server 2016 to Project Server 2019, see [Upgrade to Project Server 2019](#).

Key resources:

- [Overview of the Project Server 2019 upgrade process](#)

Get a high-level understanding of what you need to do to upgrade from Project Server 2013 to Project

Server 2016.

- [Plan for upgrade to Project Server 2019](#)

Look at planning considerations for upgrading from Project Server 2016 to Project Server 2019.

- [Things you need to know about Project Server 2019 upgrade](#)

Learn about important changes for upgrading to this version, which include:

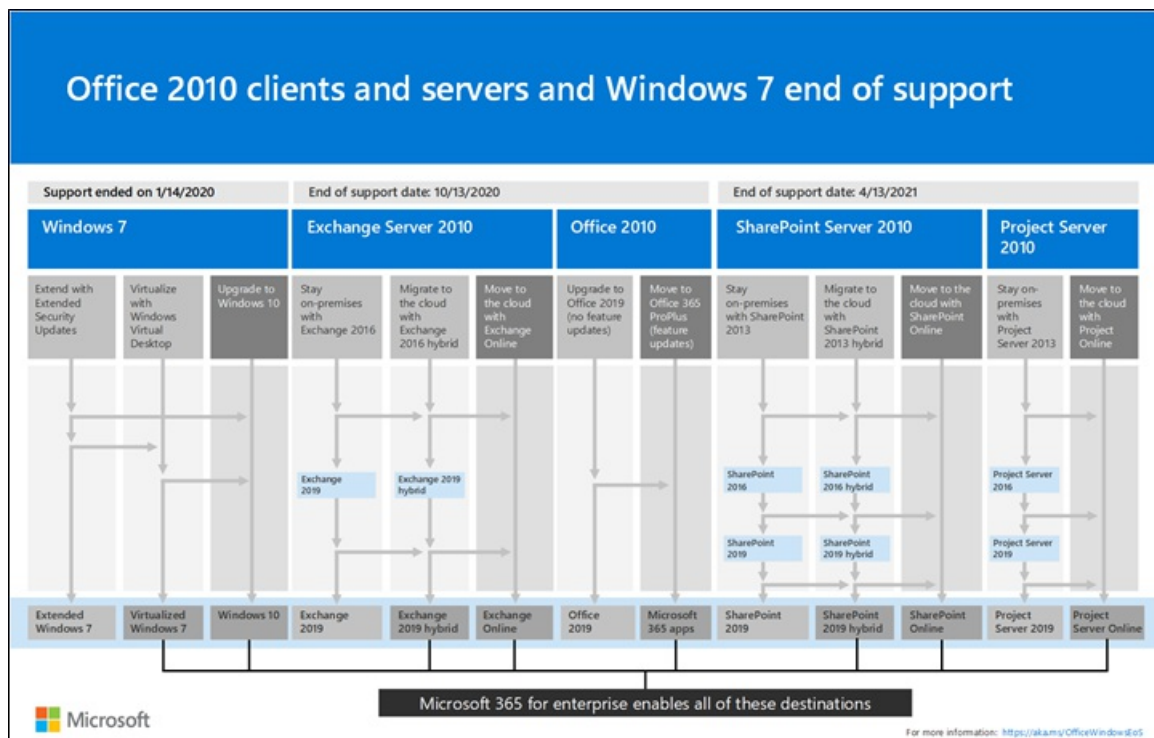
- The upgrade process will migrate your data from your Project Server 2016 database to the SharePoint Server 2019 Content database. Project Server 2019 will no longer create its own Project Server database in the SharePoint Server farm.
- After the upgrade, be aware of several changes in Project Web App. For details, see [What's new in Project Server 2019](#).

Other resources:

- [Project Online Service Descriptions](#): See the portfolio management features included with Project Server 2016 and Project Online Premium.
- [Microsoft Office Project Portfolio Server 2010 migration guide](#)

Summary of options for Office 2010 client and servers and Windows 7

For a visual summary of the upgrade, migrate, and move-to-the-cloud options for Office 2010 clients and servers and Windows 7, see the [end of support poster](#).



This poster illustrates the various paths you can take to avoid end of support for Office 2010 client and server products and Windows 7, with preferred paths and option support in Microsoft 365 Enterprise highlighted.

You can also [download](#) this poster and print it in letter, legal, or tabloid (11 x 17) format.

Related topics

[Upgrading from SharePoint 2010](#)

Resources to help you upgrade from Office 2007 servers and clients

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you're using Office 2007 products and services, be aware that support for these applications has ended. Consider moving to the Microsoft cloud, starting with Microsoft 365. Use this article as a starting point to review your options and plan your upgrade.

Office 2007 planning roadmaps

Support has ended for Office 2007 products and services. The following roadmaps can help you plan your upgrade now.

PLANNING CONTENT	DATE SUPPORT ENDED
Office 2007 end of support roadmap	October 10, 2017
Exchange 2007 end of support roadmap	April 11, 2017
SharePoint Server 2007 end of support roadmap	October 10, 2017
Project Server 2007 end of support roadmap	October 10, 2017
Upgrade from Office Communications Server	January 8, 2018
PerformancePoint Server 2007 end of support roadmap	January 9, 2018

After support ends for a Microsoft product, there are no more:

- New security updates
- New non-security updates
- Free or paid assisted support options available (including custom support agreements)
- New online technical content updates

Whether you're an enterprise organization or an individual home user, you have several options to consider.

I'm a home user. What do I do?

If you're using Office 2007 products and applications at home, see [this information](#).

Related topics

[Video: What is Microsoft 365?](#)

[Microsoft Lifecycle Policy](#)

[Plan your upgrade from Office 2007 or Office 2010 servers and clients](#)

Exchange 2007 end of support roadmap

10/28/2022 • 13 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Exchange Server 2007 reached end of support in April 2017. If you haven't started your migration from Exchange 2007 to Microsoft 365, Office 365, or Exchange 2016, now's the time to start planning.

What does *end of support* mean?

Exchange Server, like almost all Microsoft products, has a support lifecycle during which we provide new features, bug fixes, security fixes, and so on. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. Since Exchange 2007 reached its end of support on April 11, 2017, Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

Your installation of Exchange 2007 will continue to run after the end-of-support date. But because there are no new updates or support, we strongly recommend that you migrate from Exchange 2007 as soon as possible.

For more information about Office 2007 servers nearing the end of support, see [Plan your upgrade from Office 2007 servers and products](#).

What are my options?

You can:

- Migrate to Microsoft 365 by using cutover, staged, or hybrid migration.
- Migrate your Exchange 2007 servers to a newer version of Exchange on your on-premises servers.

The following sections explore each option in more detail.

Migrate to Microsoft 365

Migrating your email to Microsoft 365 is the best and simplest option to help retire your Exchange 2007 deployment. With a migration to Microsoft 365, you can make a single hop from 10-year-old technology to state-of-the-art features, including:

- Compliance capabilities such as Retention Policies, In-Place and Litigation Hold, in-place eDiscovery, and more
- Microsoft 365 Groups
- Focused Inbox
- MyAnalytics
- REST APIs for programmatic access to email, calendars, contacts, and so on

Microsoft 365 also gets new features and experiences first, so you and your users can usually start using them

right away. And you won't have to worry about:

- Purchasing and maintaining hardware.
- Paying to heat and cool your servers.
- Keeping up to date on security, product, and time-zone fixes.
- Maintaining storage and software to support compliance requirements.
- Upgrading to a new version of Exchange. With Microsoft 365, you're always on the latest version of Exchange.

How should I migrate to Microsoft 365?

You have a few migration options. You need to consider a few things, including:

- The number of seats or mailboxes you need to move.
- How long you want the migration to last.
- Whether you need seamless integration between your on-premises installation and Microsoft 365 during the migration.

This table shows your migration options and the most important factors that determine which method to use:

MIGRATION OPTION	ORGANIZATION SIZE	DURATION
Cutover migration	Fewer than 150 seats	A week or less
Staged migration	More than 150 seats	A few weeks
Full hybrid migration	Several hundred to thousands of seats	A few months or more

The following sections provide an overview of these methods. For more detail, see [Decide on a migration path](#).

Cutover migration

In a cutover migration, you migrate all your mailboxes, distribution groups, contacts, and so on, to Microsoft 365 at a preselected date and time. After the migration is complete, you shut down your on-premises Exchange servers and start using Microsoft 365 exclusively.

Cutover migration is great for small organizations that don't have many mailboxes, want to get to Microsoft 365 quickly, and don't want to deal with some of the complexities of the other methods. But it should be completed in a week or less, and it requires users to reconfigure their Outlook profiles. Cutover migration can handle up to 2,000 mailboxes, but we strongly recommend you use it to migrate a maximum of 150 mailboxes. If you try to migrate more, you could run out of time to transfer all the mailboxes before your deadline, and your IT support staff may get overwhelmed with requests to help users reconfigure Outlook.

If you're thinking about doing a cutover migration, here are things to consider:

- Microsoft 365 will need to connect to your Exchange 2007 servers using Outlook Anywhere over TCP port 443.
- All on-premises mailboxes will be moved to Microsoft 365.
- You'll need an on-premises administrator account that has read access to your users' mailboxes.
- The Exchange 2007 accepted domains that you want to use in Microsoft 365 need to be added as verified domains in the service.
- Between the time you start the migration and when you begin the completion phase, Microsoft 365 will periodically synchronize the Microsoft 365 and on-premises mailboxes. This lets you complete the

migration without worrying about email being left behind in your on-premises mailboxes.

- Users will receive new temporary passwords for their Microsoft 365 accounts. They'll need to change their password when they sign in to their mailbox for the first time.
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users will need to set up a new Outlook profile on each of their devices and download their email again. The amount of email that Outlook will download can vary. For more information, see [Change how much mail to keep offline](#).

For more information about cutover migration, see:

- [What you need to know about a cutover email migration](#)
- [Perform a cutover migration of email](#)

Staged migration

In a staged migration, you have a few hundred or a few thousand mailboxes that you want to migrate to Microsoft 365, need to take a week or more to complete the migration, and don't need any of advanced hybrid migration features like shared Free/Busy calendar information.

Staged migration is great for organizations that need to take more time to migrate their mailboxes to Microsoft 365 but still plan to complete the migration within a few weeks. You can migrate mailboxes in batches. You control how many and which mailboxes are migrated at a given time. You might batch mailboxes of users in the same department, for example, to make sure they're all moved at the same time. Or, you might leave executive mailboxes until the last batch. As with cutover migrations, your users will need to recreate their Outlook profiles.

If you're thinking about doing a staged migration, here are things to consider:

- Microsoft 365 will need to connect to your Exchange 2007 servers by using Outlook Anywhere over TCP port 443.
- You'll need an on-premises administrator account that has read access to your users' mailboxes.
- The Exchange 2007 accepted domains that you plan to use in Microsoft 365 need to be added as verified domains in the service.
- You'll need to create a CSV file with the full name and email address of each mailbox that you plan to migrate in a batch. You'll also need to include a new password for each mailbox that you're migrating, and send that password to each user. The user will be prompted to change the password the first time that they sign in to their new Microsoft 365 mailbox.
- Between the time you start the migration batch and when you begin the completion phase, Microsoft 365 will periodically synchronize the Microsoft 365 and on-premises mailboxes included in the batch. This lets you complete the migration without worrying about email being left behind in your on-premises mailboxes.
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users will need to set up a new Outlook profile on each of their devices and download their email again. The amount of email that Outlook will download can vary. For more information, see [Change how much mail to keep offline](#).

For more information about staged migration, see:

- [What you need to know about a staged email migration](#)
- [Perform a staged migration of email](#)

Full hybrid

In a full hybrid migration, your organization has many hundreds, up to tens of thousands, of mailboxes, and you want to move some or all of them to Microsoft 365. Because these migrations are typically longer-term, hybrid migrations make it possible to:

- Show on-premises users the free/busy calendar information for users in Microsoft 365, and vice versa.
- See a unified global address list that contains recipients in both on-premises and Microsoft 365.
- View full Outlook recipient properties for all users, regardless of whether they're on-premises or in Microsoft 365.
- Secure email communication between on-premises Exchange servers and Microsoft 365 using TLS and certificates.
- Treat messages sent between on-premises Exchange servers and Microsoft 365 as internal, enabling them to:
 - Be properly evaluated and processed by transport and compliance agents targeting internal messages.
 - Bypass anti-spam filters.

Full hybrid migration is best for organizations that expect to stay in a hybrid configuration for many months or more. You'll get the features listed earlier in this section, plus directory synchronization, better integrated compliance features, and the ability to move mailboxes to and from Microsoft 365 by using online mailbox moves. Microsoft 365 becomes an extension of your on-premises organization.

If you're thinking about doing a full hybrid migration, here are things to consider:

- Full hybrid migration isn't suited to all types of organizations. Due to the complexity of full hybrid migrations, organizations with less than a few hundred mailboxes don't typically see benefits that justify the effort and cost needed to set one up. If this sounds like your organization, we recommend that you consider a cutover or staged migration instead.
- You'll need to deploy at least one Exchange 2013 server in your Exchange 2007 organization to act as a "hybrid server." This server will communicate with Microsoft 365 on behalf of your Exchange 2007 servers.
- Microsoft 365 will need to connect to the "hybrid server" using Outlook Anywhere over TCP port 443.
- You'll need to set up directory synchronization using Azure Active Directory (Azure AD) Connect between your on-premises Active Directory servers and Microsoft 365.
- Users will be able to sign in to their Microsoft 365 mailbox using the same user name and password as when they sign in to the local network. (This functionality requires Azure AD Connect with password synchronization and/or Active Directory Federation Services.)
- You'll need a Microsoft 365 license that includes Exchange Online for each user mailbox you migrate.
- Users don't need to set up a new Outlook profile on most of their devices, although some older Android phones might need a new profile. Users won't have to redownload their email.

If full hybrid migration sounds right for you, see the following resources to help with your migration:

- [Exchange Deployment Assistant](#)
- [Exchange Server Hybrid Deployments](#)
- [Hybrid Configuration wizard](#)
- [Hybrid Configuration wizard FAQs](#)

- [Hybrid deployment prerequisites](#)

Migrate to a newer version of Exchange Server

We strongly believe that you can achieve the best value and user experience by migrating to Microsoft 365. But we also understand that some organizations need to keep their email on-premises. This could be because of regulatory requirements, to guarantee data isn't stored in a datacenter located in another country, or similar. If you choose to keep your email on-premises, you can migrate your Exchange 2007 environment to Exchange 2010, Exchange 2013, or Exchange 2016.

If you can't migrate to Microsoft 365, we recommend that you migrate to Exchange 2016. Exchange 2016 includes all the features of previous releases of Exchange. It also most closely matches the experience available with Microsoft 365, although some features are available only in Microsoft 365. Check out just a few of the things you've been missing:

EXCHANGE RELEASE	FEATURES
Exchange 2010	Role-Based Access Control (permissions without ACLs) Outlook Web App mailbox policies Ability to share free/busy and delegate calendars between organizations
Exchange 2013	<i>Features from Exchange 2010 and ...</i> Simplified architecture that reduced the number of server roles to three (Mailbox, Client Access, Edge Transport) Data loss prevention policies (DLP) that help keep sensitive information from leaking Improved Outlook Web App experience
Exchange 2016	<i>Features from Exchange 2013 and ...</i> Further simplified server roles to just Mailbox and Edge Transport Improved DLP along with integration with SharePoint Improved database resilience Online document collaboration

Which version should I migrate to?

We recommend that you initially assume that you'll migrate to Exchange 2016. Then, use the following information to confirm your assumption or to rule out Exchange 2016. If you can't migrate to Exchange 2016 for some reason, do the same process with Exchange 2013, and so on.

CONSIDERATION	MORE INFO
End of support dates	Like Exchange 2007, each version of Exchange has its own end-of-support date: <i>Exchange 2010</i> - January 2020 <i>Exchange 2013</i> - April 2023 <i>Exchange 2016</i> - October 2025 The earlier the end of support, the sooner you'll need to perform another migration.

CONSIDERATION	MORE INFO
Migration path to Exchange 2010 and 2013.	Here are the general phases for migrating to Exchange 2010 or Exchange 2013: - Install Exchange 2010 or 2013 into your existing Exchange 2007 organization. - Move services and other infrastructure to Exchange 2010 or 2013. - Move mailboxes and public folders to Exchange 2010 or 2013. - Decommission remaining Exchange 2007 servers.
Migration path to Exchange 2016	Here are the general phases for migrating to Exchange 2016: - Install Exchange 2013 into your existing Exchange 2007 organization. - Move services and other infrastructure to Exchange 2013. - Move mailboxes and public folders to Exchange 2013. - Decommission remaining Exchange 2007 servers. - Install Exchange 2016 into your existing Exchange 2013 organization. - Move mailboxes, public folders, services, and other infrastructure to Exchange 2016 (order doesn't matter). - Decommission remaining Exchange 2013 servers. Note: Migrating from Exchange 2013 to Exchange 2016 is simple. The two versions have almost the same hardware requirements, and these versions are very compatible. So you can rebuild a server you bought for Exchange 2013 and install Exchange 2016 on it. For online mailbox moves, most users won't even notice that their mailbox was moved off the server and then back after you've rebuilt it with Exchange 2016.
Version coexistence	When migrating to ... Exchange 2016: Exchange 2016 can't be installed in an organization that includes an Exchange 2007 server. You'll first need to migrate to Exchange 2010 or 2013 (we strongly recommend Exchange 2013), remove all Exchange 2007 servers, and then migrate to Exchange 2016. Exchange 2010 or Exchange 2013: You can install Exchange 2010 or Exchange 2013 into an existing Exchange 2007 organization. This enables you to install one or more Exchange 2010 or 2013 servers and perform your migration.
Server hardware	Server hardware requirements have changed from Exchange 2007. Make sure your hardware is compatible. For details, see: Exchange 2016 System Requirements Exchange 2013 System Requirements Exchange 2010 System Requirements You'll find that the significant improvements in Exchange performance and the increased computing power and storage capacity in newer servers mean you'll likely need fewer servers to support the same number of mailboxes.

CONSIDERATION	MORE INFO
Operating system version	The minimum supported operating system versions for each version are: Exchange 2016 - Windows Server 2012 Exchange 2013 - Windows Server 2008 R2 SP1 Exchange 2010 - Windows Server 2008 SP2 Find more information about operating system support at Exchange Supportability Matrix.
Active Directory forest functional level	The minimum supported Active Directory forest functional levels for each version are: Exchange 2016 Windows Server 2008 R2 SP1 Exchange 2013 Windows Server 2003 Exchange 2010 Windows Server 2003 Find more information about forest functional level support at Exchange Supportability Matrix.
Office client versions	The minimum supported Office client versions for each version are: Exchange 2016 - Office 2010 (with the latest updates) Exchange 2013 - Office 2007 SP3 Exchange 2010 - Office 2003 Find more information about Office client support at Exchange Supportability Matrix.

How do I migrate?

If you decided to keep your email on-premises, use the following resources to help with your migration:

- [Exchange Deployment Assistant](#)
- Active Directory schema changes for Exchange [2016](#), [2013](#), [2010](#)
- System requirements for Exchange [2016](#), [2013](#), [2010](#)
- Prerequisites for Exchange [2016](#), [2013](#), [2010](#)

Get help

If you're migrating to Microsoft 365, you might be eligible to use our Microsoft FastTrack service. FastTrack provides best practices, tools, and resources to make your migration to Microsoft 365 as seamless as possible. Best of all, a support engineer will walk you through your migration, from planning and design all the way to migrating your last mailbox. For more about FastTrack, see [Microsoft FastTrack](#).

If you run into problems during your migration to Microsoft 365 and you aren't using FastTrack, or your migration to a newer version of Exchange Server, we're here to help. Here are some resources you can use:

- [Technical community](#)
- [Customer support](#)

Related topics

[Resources to help you upgrade your Office 2007 servers and clients](#)

SharePoint Server 2007 end of support roadmap

10/28/2022 • 12 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

On **October 10, 2017**, Microsoft Office SharePoint Server 2007 reached end of support. If you haven't migrated from SharePoint Server 2007 to Microsoft 365 or a newer version of SharePoint Server on-premises, now's the time to start planning. This article provides resources to help you migrate data to SharePoint Online or upgrade your SharePoint Server on-premises.

What does *end of support* mean?

SharePoint Server, like most Microsoft products, has a support lifecycle, during which Microsoft provides new features, bug fixes, security fixes, and so on. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. After the end of support, Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

Your SharePoint Server 2007 farm will still be operational after October 10, 2017, but no further updates, patches, or fixes will be released for the product, including security patches/fixes. Microsoft Support has fully shifted its support efforts to more-recent versions of the product. Because your installation is no longer supported or patched, you should upgrade the product or migrate important data.

TIP

If you haven't already planned for upgrade or migration, see: [SharePoint 2007 migration options to consider](#) for some examples of where to begin. You can also search for [Microsoft Partners](#) who can help with upgrade or Microsoft 365 migration (or both).

For more information about Office 2007 servers and the end of support, see [Resources to help you upgrade from Office 2007 servers and clients](#).

What are my options?

Your first stop should be the [Product Lifecycle site](#). If you have an on-premises Microsoft product that's aging, check its end of support date so that you have a year or so to schedule an upgrade or migration. When you choose the next step, consider what product features would be good enough, better, and best. Here's an example:

GOOD	BETTER	BEST
SharePoint Server 2010	SharePoint Server 2013	SharePoint Online
	SharePoint Hybrid	SharePoint Server 2016

GOOD	BETTER	BEST
		SharePoint Hybrid

If you choose a "good enough" option, you'll soon need to begin planning for another upgrade after migration from SharePoint Server 2007 is completed.

NOTE

End-of-support dates are subject to change. Check the [Product Lifecycle site](#).

Where can I go next?

SharePoint Server can be installed on-premises on your own servers. Or you can use SharePoint Online, which is an online service that's part of Microsoft 365. Your options are:

- Migrate to SharePoint Online.
- Upgrade SharePoint Server on-premises.
- Do both of the above.
- Implement a [SharePoint hybrid](#) solution.

Be aware of hidden costs associated with maintaining a server farm, maintaining or migrating customizations, and upgrading the hardware that SharePoint Server needs. Having an on-premises SharePoint Server farm is rewarding if it's necessary. But if you run your farm on legacy SharePoint Servers without heavy customization, you can benefit from migration to SharePoint Online.

IMPORTANT

There's another option if the content in SharePoint 2007 is infrequently used. Some SharePoint Administrators choose to create a Microsoft 365 subscription, set up a new SharePoint Online site, and then cut away from SharePoint 2007 cleanly, taking only essential documents to the fresh SharePoint Online sites. Data can then be drained from the SharePoint 2007 site into archives. Consider how your users work with data from your SharePoint 2007 installation. There may be creative ways to manage your needs.

SHAREPOINT ONLINE (SPO)	SHAREPOINT SERVER ON-PREMISES
High cost in time (plan / execution/verification)	High cost in time (plan / execution/verification)
Lower cost in funds (no hardware purchases)	Higher cost in funds (hardware + devs/admins)
One-time cost in migration	One-time cost repeated per future migration
Low total cost of ownership/maintenance	High total cost of ownership/maintenance

When you migrate to Microsoft 365, the one-time move will have a heavier cost up-front, while you organize data and decide what to take to the cloud and what to leave behind. But future upgrades will be automatic, and you'll no longer need to manage hardware and software updates. Also, the up time of your farm will be backed by a Microsoft Service Level Agreement ([SLA](#)).

Migrate to SharePoint Online

Make sure that SharePoint Online has all the features you need. See [Microsoft 365 and Office 365 service](#)

[descriptions.](#)

You can't migrate directly from SharePoint 2007 to SharePoint Online. Your move to SharePoint Online would be done manually. If you upgrade to SharePoint Server 2013 or SharePoint Server 2016, you might use the SharePoint Migration API (to migrate information into OneDrive for Business, for example).

ONLINE PRO	ONLINE CON
Microsoft supplies SPO hardware and all hardware administration.	Available features may differ between SharePoint Server on-premises and SPO.
You're the SharePoint admin or global admin of your subscription and can assign administrators to SPO sites.	Some actions available to a farm administrator in SharePoint Server on-premises don't exist or aren't necessarily included in the SharePoint Administrator role in Microsoft 365.
Microsoft applies patches, fixes, and updates to underlying hardware and software.	Because there's no access to the underlying file system in the service, customization is limited.
Microsoft publishes Service level agreements and moves quickly to resolve service-level incidents.	Backup and restore and other recovery options are automated by the service in SharePoint Online. Backups are overwritten if not used.
Security testing and server performance tuning are carried out on an ongoing basis in the service by Microsoft.	Changes to the user interface and other SharePoint features are installed by the service and may need to be toggled on or off.
Microsoft 365 meets many industry standards: Microsoft compliance offerings .	FastTrack assistance for migration is limited. Much of the upgrade will be manual or via the SPO Migration API described in the SharePoint Online and OneDrive Migration Content Roadmap .
Microsoft Support engineers and datacenter employees won't have unrestricted admin access to your subscription.	There can be additional costs if hardware needs to be upgraded to support the newer version of SharePoint, or if a secondary farm is required for upgrade.
Partners can assist with the one-time job of migrating your data to SharePoint Online.	
Online products are updated automatically. Although features may deprecate, there's no true end of support.	

If you've decided to create a new Microsoft 365 site and will manually migrate data to it as is needed, check your [Microsoft 365 options](#).

Upgrade SharePoint Server on-premises

There's no way to skip versions in SharePoint Upgrades. Upgrades go serially:

- SharePoint 2007 > SharePoint Server 2010 > SharePoint Server 2013 > SharePoint Server 2016

To go from SharePoint 2007 to SharePoint Server 2016 means a significant investment of time and will involve costs in hardware (SQL servers must also be upgraded), software, and administration. Customizations will need to be upgraded or abandoned.

NOTE

It's possible to maintain your end-of-life SharePoint 2007 farm, install a SharePoint Server 2016 farm on new hardware (so the separate farms run side-by-side), and then plan and execute a manual migration of content (for downloading and re-uploading content, for example). But beware of some of the pitfalls of manual moves, such as moves of documents replacing the last-modified account with the alias of the account doing the manual move. Also consider the work that must be done ahead of time, such as recreating sites, subsites, permissions, and list structures. Consider in advance what data you can move into storage or delete to reduce the impact of migration.

It's important to clean up your environment before you upgrade. Be certain your existing farm is functional before you upgrade, and certainly before you decommission!

Remember to review the *supported and unsupported upgrade paths*:

- [SharePoint Server 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

If you have customizations, it's critical to have a plan for each step in the migration path:

- [SharePoint 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

ON-PREMISES PRO	ON-PREMISES CON
Full control of all aspects of your SharePoint Farm, from the server hardware up.	All breaks and fixes are the responsibility of your company (you can engage paid Microsoft Support if your product is not past end of support).
Full feature set of SharePoint Server on-premises with the option to connect your on-premises farm to a SharePoint Online subscription via hybrid.	Upgrade, patches, security fixes, and all maintenance of SharePoint Server managed on-premises.
Full access for greater customization.	Microsoft compliance offerings must be manually configured on-premises.
Security testing, and server performance tuning is carried out on your premises (under your control).	Microsoft 365 may make features available to SharePoint Online that don't interoperate with SharePoint Server on-premises.
Partners can assist with migrating data to the next version of SharePoint Server (and beyond).	Your SharePoint Server sites won't automatically use SSL/TLS certificates as is seen in SharePoint Online.
Full control of naming conventions, back up and restore, and other recovery options in SharePoint Server on-premises.	SharePoint Server on-premises is sensitive to product lifecycles.

Upgrade resources

Make sure your environment meets hardware and software requirements, and then follow supported upgrade methods.

- **Hardware/software requirements for:**

[SharePoint Server 2010](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- **Software boundaries and limits for:**

[SharePoint Server 2007](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- **The upgrade process overview for:**

[SharePoint Server 2007](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

Create a SharePoint hybrid solution between SharePoint Online and on-premises

If the answer to your migration needs is somewhere between the self-control offered by on-premises and the lower cost of ownership offered by SharePoint Online, you can connect SharePoint Server 2013 or 2016 farms to SharePoint Online through hybrids. [Learn about SharePoint hybrid solutions.](#)

If you decide that a hybrid SharePoint Server farm will benefit your business, familiarize yourself with the existing types of hybrids and how to configure the connection between your on-premises SharePoint farm and your Microsoft 365 subscription.

OPTION	DESCRIPTION
Microsoft compliance offerings	FastTrack assistance for migration is limited. Much of the upgrade will be manual, or via the SPO Migration API described in the SharePoint Online and OneDrive Migration Content Roadmap .
Microsoft Support engineers and data center employees don't have unrestricted admin access to your subscription.	There can be additional costs if hardware infrastructure needs to be upgraded to support the newer version of SharePoint, or if a secondary farm is required for upgrade.
Partners can assist with the one-time job of migrating your data to SharePoint Online.	
Online products are updated automatically across the service. Though features may deprecate, there's no true end of support.	

If you've decided to create a new Microsoft 365 site and will manually migrate data to it as is needed, check your [Microsoft 365 options](#).

Upgrade SharePoint Server on-premises

There's no way to skip versions in SharePoint Upgrades. Upgrades go serially:

- SharePoint 2007 > SharePoint Server 2010 > SharePoint Server 2013 > SharePoint Server 2016

To go from SharePoint 2007 to SharePoint Server 2016 will mean a significant investment of time and will involve costs for hardware (SQL servers must also be upgraded), software, and administration. Customizations will need to be upgraded or abandoned.

NOTE

It's possible to maintain your end-of-life SharePoint 2007 farm, install a SharePoint Server 2016 farm on new hardware (so the separate farms run side-by-side), and then plan and execute a manual migration of content (for downloading and re-uploading content, for example). But beware of potential pitfalls of manual moves, such as moves of documents replacing the last-modified account with the alias of the account doing the manual move, and the work that must be done ahead of time, such as recreating sites, subsites, permissions and list structures. Consider what data you can move into storage or delete to reduce the impact of migration.

Clean your environment prior to upgrade. Be certain your existing farm is functional before you upgrade and

certainly before you decommission!

Remember to review the *supported and unsupported upgrade paths*:

- [SharePoint Server 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

If you have *customizations*, it's critical you have a plan your upgrade for each step in the migration path:

- [SharePoint 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)

ON-PREMISES PRO	ON-PREMISES CON
Full control of all aspects of your SharePoint Farm, from the server hardware up.	All breaks and fixes are the responsibility of your company. (You can engage paid Microsoft Support if your product isn't past end of support.)
Full feature set of SharePoint Server on-premises with the option to connect your on-premises farm to a SharePoint Online subscription via hybrid.	Upgrade, patches, security fixes, and all maintenance of SharePoint Server managed on-premises.
Full access for greater customization.	Microsoft compliance offerings must be manually configured on-premises.
Security testing and server performance tuning are carried out on your premises under your control.	Microsoft 365 may make features available to SharePoint Online that don't interoperate with SharePoint Server on-premises
Partners can help migrate data to the next version of SharePoint Server (and beyond).	Your SharePoint Server sites will not automatically use SSL/TLS certificates as is seen in SharePoint Online.
Full control of naming conventions, back up and restore, and other recovery options in SharePoint Server on-premises.	SharePoint Server on-premises is sensitive to product lifecycles.

Upgrade resources

Make sure that your environment meets hardware and software requirements. Then follow the supported upgrade methods.

- **Hardware/software requirements for:**

[SharePoint Server 2010](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- **Software boundaries and limits for:**

[SharePoint Server 2007](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

- **The upgrade process overview for:**

[SharePoint Server 2007](#) | [SharePoint Server 2010](#) | [SharePoint Server 2013](#) | [SharePoint Server 2016](#)

Create a SharePoint hybrid solution between SharePoint Online and on-premises

If the answer to your migration needs is somewhere between the self-control offered by on-premises and the lower cost of ownership offered by SharePoint Online, you can connect SharePoint Server 2013 or 2016 farms

to SharePoint Online through hybrids. [Learn about SharePoint hybrid solutions](#)

If you decide that a hybrid SharePoint Server farm will benefit your business, familiarize yourself with the existing types of hybrids and how to configure the connection between your on-premises SharePoint farm and your Microsoft 365 subscription.

One good way to see how this works is to create a Microsoft 365 dev/test environment, which you can set up with [Test Lab Guides](#). After you get a trial or purchased Microsoft 365 subscription, you can create the site collections, webs, and document libraries in SharePoint Online to which you can migrate data. You can migrate manually, by use of the Migration API, or, if you want to migrate My Site content to OneDrive for Business, through the hybrid wizard.

NOTE

Remember that to use the hybrid option, your SharePoint 2007 farm will need to be upgraded, on-premises, to either SharePoint Server 2013 or SharePoint Server 2016.

Related topics

[Troubleshoot and resume upgrade \(Office SharePoint Server 2007\)](#)

[Troubleshoot upgrade issues \(SharePoint Server 2010\)](#)

[Troubleshoot database upgrade issues in SharePoint 2013](#)

[Search for Microsoft Partners to help with Upgrade](#)

[Resources to help you upgrade from Office 2007 servers and clients](#)

PerformancePoint Server 2007 end of support roadmap

10/28/2022 • 9 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Office 2007 servers and applications have reached their end of support, including servers and applications that you might be using as part of your business intelligence (BI) solutions. The following table lists BI applications that are affected:

MICROSOFT BI APPLICATIONS	DATE SUPPORT ENDED
ProClarity Analytics Server 6.3 Service Pack 3 ProClarity Desktop Professional 6.3 ProClarity SharePoint Viewer 6.3	July 11, 2017
SharePoint Server 2007 Service Pack 3	October 10, 2017
PerformancePoint Server 2007 Service Pack 3	January 9, 2018

For more information, see [Resources to help you upgrade from Office 2007 servers and clients](#).

What does *end of support* mean?

Like most Microsoft products, PerformancePoint Server 2007 SP3, ProClarity software, and SharePoint Server 2007 SP3, have a support lifecycle, during which Microsoft provides new features, bug fixes, and security updates. The lifecycle for a product typically lasts for 10 years from the product's initial release. The end of that lifecycle is known as the product's end of support. As ProClarity, PerformancePoint Server, and SharePoint Server 2007 have reached their end of support, Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that are discovered and that may impact the stability and usability of servers.
- Security fixes for vulnerabilities that are discovered and that may make servers or applications vulnerable to security breaches.
- Time zone updates.

Your installation of ProClarity, SharePoint Server 2007 SP3, and PerformancePoint Server 2007 SP3 will continue to run even though support has ended. However, we strongly recommend that you migrate from these applications as soon as possible.

What are my options?

There have been lots of changes to Microsoft BI applications since 2007, and you have several options to consider, as summarized in the following table.

IF YOU WERE USING THIS ...	EXPLORE THESE OPTIONS ...	AND KEEP THIS IN MIND ...
PerformancePoint Server 2007 Monitoring & Analytics capabilities, including: - PerformancePoint Monitoring Server - PerformancePoint Dashboard Designer - Dashboard Viewer for SharePoint Services (used for rendering PerformancePoint dashboards, scorecards, and reports)	Excel with Excel in a browser (in the cloud or on-premises). For an overview, see BI capabilities in Excel and Microsoft 365. Power BI (in the cloud or on-premises). For an overview, see What is Power BI? SQL Server Reporting Services (on-premises). For an overview, see SQL Server Reporting Services (SSRS): Create, deploy, and manage mobile and paginated reports. PerformancePoint Services (on-premises). For an overview, see What's new for PerformancePoint Services (SharePoint Server 2010).	Excel is available as an online (cloud-based) or on-premises solution. Many reporting and dashboard needs can be met with Excel. Power BI is available as an online or on-premises solution. Power BI isn't included in Microsoft 365. But you can start using Power BI for free. Later, depending on your data usage and business needs, you can upgrade to Power BI Pro with Microsoft 365 E5. Reporting Services and PerformancePoint Services are both on-premises solutions. PerformancePoint Services is available in SharePoint Server 2010, SharePoint Server 2013, and SharePoint Server 2016. Some features and report types that were available in PerformancePoint Server 2007 aren't available in Excel, Power BI, Reporting Services, or PerformancePoint Services. Review the available features to determine the best solution for your business needs.
ProClarity software, including: - ProClarity Desktop Professional - ProClarity Analytics Server - ProClarity SharePoint Viewer	Work with a Microsoft partner to identify a solution that best meets your needs. Visit the Microsoft Partner Center. You can also consider using Excel with Excel in a browser, Power BI, SQL Server Reporting Services, or PerformancePoint Services.	Several but not all features of ProClarity software are available in other Microsoft offerings, including Excel, Power BI, Reporting Services, and PerformancePoint Services.
SharePoint Server 2007 KPIs (also called MOSS KPIs)	Excel with Excel Services. For an overview, see Business intelligence in Excel and Excel Services (SharePoint Server 2013).	MOSS KPIs that were created using SharePoint Server 2007 can be used in SharePoint Server 2010, SharePoint Server 2013, and SharePoint Server 2016. But you can't create new MOSS KPIs.
Excel 2007	Excel (in the cloud or on-premises). For an overview, see BI capabilities in Excel and Office 365. Power BI (in the cloud or on-premises). For an overview, see What is Power BI?	Both Excel and Power BI offer your organization cloud-based and on-premises solutions, with support for a wide variety of data sources.

Help selecting a solution

With so many BI choices available, it might seem overwhelming to determine which option is best. We have an online guide available to help. See [Choosing Microsoft Business Intelligence \(BI\) tools for analysis and reporting](#).

What if I don't upgrade now?

You can choose to not upgrade immediately. Your existing servers and applications will continue to run. But you won't receive any further updates, including security updates, since support has ended. And if something goes wrong with your server applications you won't be able to get help from Microsoft technical support.

How do I plan my upgrade?

After you explore your upgrade options, the next step is to prepare an upgrade plan. The following sections include information and additional resources to help. You have four main options, including two that work both in the cloud or on-premises, and two that are on-premises-only:

OPTION	IN THE CLOUD OR ON-PREMISES?
Excel with SharePoint Server (on-premises)	Both
Power BI	Both
Reporting Services	On-premises only
PerformancePoint Services	On-premises only

Use Excel (in the cloud or on-premises)

With Excel, which is also known as *Excel Services* in SharePoint Server, you can view and use workbooks in a browser window, even if Excel isn't installed on the computer. You can use Excel to create reports, scorecards, and dashboards. Then, share your workbooks with others, who can use Excel in a browser, whether they're using SharePoint Online as part of Microsoft 365 or SharePoint Server on-premises. You can use data stored on-premises or in the cloud, which enables you to use a wide variety of data sources.

The following table compares key advantages of using Excel with Microsoft 365 to using Excel with SharePoint Server. More information follows.

EXCEL WITH MICROSOFT 365 (IN THE CLOUD)	EXCEL WITH SHAREPOINT SERVER (ON-PREMISES)
You get the latest, greatest version of Excel. With Microsoft 365, you get the latest version of Excel, which includes powerful new chart types, the ability to create charts and tables quickly and easily, and support for more data sources. Setup is much simpler. Excel is included with Microsoft 365 for business, so there's no heavy lifting on your part. Sign up and sign in, and you'll be up and running faster and more efficiently than if you upgrade your on-premises servers. People have everywhere access to their workbooks. People can securely view workbooks from wherever they are, using their computer, smart phone, and tablet. There's more! See BI capabilities in Excel and Office 365.	You manage your global settings. As a SharePoint administrator, you can specify global settings, such as security, load balancing, session management, workbook caching, and external data connections. You can use Excel Services with PerformancePoint Services. You can configure Excel Services and PerformancePoint Services as part of your SharePoint Server installation, and include Excel Services reports in your PerformancePoint dashboards. There's more! See Business intelligence in Excel and Excel Services (SharePoint Server 2013).

Excel with Microsoft 365 (in the cloud)

If you move to Microsoft 365, you'll have the most up-to-date services and applications, including Excel 2016. PerformancePoint Services isn't available in Microsoft 365, so you'll be replacing your PerformancePoint dashboard content with Excel workbooks or other reports. The good news is that Excel 2016 has lots of new chart types, and it's easier than ever to create impressive dashboards in Excel. And new features are added

regularly. To learn more, see [What's New in Excel 2016 for Windows](#).

Also, if you purchase 50 seats or more of Microsoft 365, the Microsoft FastTrack team can help you get set up. To learn more, visit [FastTrack](#).

Excel with SharePoint Server (on-premises)

If you upgrade to a newer version of SharePoint, you can use Excel with Excel Services or in a browser, as follows:

- Excel Services in SharePoint Server 2010
- Excel Services in SharePoint Server 2013
- Excel, which is part of Office Online Server, installed separately from SharePoint Server 2016

You can configure PerformancePoint Services in your new version of SharePoint Server as well, and use that together with Excel.

To learn more about your SharePoint upgrade options, see [SharePoint Server 2007 end of support Roadmap](#).

To learn more about Excel Services, see [Excel Services overview \(SharePoint Server 2010\)](#).

Use Power BI (in the cloud or on-premises)

Power BI is a suite of business analytics tools to analyze data and share insights. With Power BI, you can use on-premises or online data sources to create interactive reports and dashboards. People can view and use your reports and dashboards on their computers or mobile devices.

Power BI isn't part of Microsoft 365 or SharePoint Server. It's a separate offering that includes Power BI Desktop, Power BI gateways, and the Power BI service. Power BI also integrates with SharePoint Online. You can get started with Power BI for free. Based on your data usage and business needs, you can later upgrade to Power BI Pro with Microsoft 365 E5. To learn more, see [What is Power BI?](#)

Use Reporting Services (on-premises)

SQL Server Reporting Services provides a robust reporting solution. You can configure Reporting Services in either native mode or SharePoint-integrated mode. You can use several different tools to author reports, including Report Designer, Report Builder, and Power View. With the latest release of SQL Server, you can also use SQL Server Mobile Report Publisher to deliver reports that scale to any screen size. This lets viewers consume reports on their mobile devices. To learn more, see [SQL Server Reporting Services \(SSRS\): Create, deploy, and manage mobile and paginated reports](#).

Use PerformancePoint Services (on-premises)

PerformancePoint Server 2007 was sold separately from SharePoint Server 2007. Beginning with SharePoint Server 2010, PerformancePoint Services is a service application in SharePoint Server. So, you don't have to purchase separate server licenses or hardware to use PerformancePoint Services.

To move from PerformancePoint Server 2007 to PerformancePoint Services, you move to a more recent version of SharePoint Server and configure PerformancePoint Services. The version of SharePoint Server that you move to determines whether you can import your existing dashboard content from PerformancePoint Server 2007 to PerformancePoint Services.

- If you upgrade to SharePoint Server 2010, you can import your PerformancePoint dashboard content from PerformancePoint Server 2007 to PerformancePoint Services in SharePoint Server 2010. To learn more, see [Import Wizard: PerformancePoint Server 2007 content to SharePoint Server 2010](#).
- If you move to SharePoint Server 2013 or SharePoint Server 2016, you'll most likely need to create new dashboard content (data sources, reports, scorecards, and dashboard pages).

To get started on your PerformancePoint Services upgrade plan, see the following resources:

- [SharePoint Server 2007 end of support Roadmap](#)
- When you know which version of SharePoint you're moving to, see the corresponding article for PerformancePoint Services:
 - [Plan for PerformancePoint Services \(SharePoint Server 2010\)](#)
 - [PerformancePoint Services in SharePoint Server 2013 overview](#)
 - [PerformancePoint Services in SharePoint Server 2016 overview](#)

When you upgrade to PerformancePoint Services, you get several new features and enhancements. PerformancePoint Services offers improved scorecards; new visualizations, such as the Decomposition Tree and KPI Details report; more chart types; better Time Intelligence filtering capabilities; and improved accessibility compliance. To learn more, see [What's new for PerformancePoint Services \(SharePoint Server 2010\)](#).

Where can I get help with my upgrade?

Whether you upgrade on-premises or move to Microsoft 365, we recommend that you work with a Microsoft partner. A qualified partner can help you identify the solution that best meets your business needs and help with your deployment. Visit the [Microsoft Partner Center](#), and use the search filters to find a solution provider.

Related topics

[Resources to help you upgrade from Office 2007 servers and clients](#)

Project Server 2007 end of support roadmap

10/28/2022 • 9 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Support ended for Office 2007 servers and applications in 2017, and you need to consider plans for migration. If you're currently using Project Server 2007 and related products, note the following end-of-support dates:

PRODUCT	END OF SUPPORT DATE
Project Server 2007	October 10, 2017
Project Portfolio Server 2007	October 10, 2017
Project 2007 Standard	October 10, 2017
Project 2007 Professional	October 10, 2017

For more information about Office 2007 servers reaching retirement, see [Upgrade from Office 2007 servers and client products](#).

What does *end of support* mean?

Most Microsoft products have a support lifecycle during which they get new features, bug fixes, security fixes, and so on. This lifecycle typically lasts for 10 years from the product's initial release. The end of this lifecycle is known as the product's end of support. Because Project Server 2007 reached its end of support on October 10, 2017, Microsoft no longer provides:

- Technical support for problems that may occur.
- Bug fixes for issues that may impact the stability and usability of the server.
- Security fixes for vulnerabilities that may make the server vulnerable to security breaches.
- Time zone updates.

Your installation of Project Server 2007 will continue to run after this date. But because of the changes listed previously, we strongly recommend that you migrate from Project Server 2007 as soon as practical.

What are my options?

If you're using Project Server 2007, you need to explore your migration options, which are:

- Migrate to Project Online
- Migrate to a newer on-premises version of Project Server (preferably Project Server 2016)

WHY WOULD I PREFER TO MIGRATE TO PROJECT ONLINE	WHY WOULD I PREFER TO MIGRATE TO PROJECT SERVER 2016
I have mobile users. Costs to migrate are a significant concern (hardware, software, hours, and effort to implement). After migration, costs to maintain my environment are a major concern (for example, automatic updates, guaranteed uptime, and so on).	Business rules restrict me from operating my business in the cloud. I need control of updates to my environment.

NOTE

For more information about options for moving from your Office 2007 servers, see [Resources to help you upgrade from Office 2007 servers and clients](#). Note that Project Server doesn't support a hybrid configuration, because Project Server and Project Online can't share the same resource pool.

Important considerations when you migrate from Project Server 2007

Consider the following when you plan to migrate from Project Server 2007:

- **Get help from a Microsoft Partner** - Upgrading from Project Server 2007 can be challenging and requires much preparation and planning. It might be especially challenging if you weren't the person who set up Project Server 2007 originally. Fortunately, there are Microsoft Partners who can help, whether you plan to migrate to Project Server 2016 or to Project Online. Search for a Microsoft Partner to help with your migration on the [Microsoft Partner Center](#). Search on the term *Gold Project and Portfolio Management* to view a list of all Microsoft Partners who have expertise in Project.
- **Plan for your customizations** - Many of the customizations you made in your Project Server 2007 environment might not work when you migrate to Project Server 2016 or Project Online. There are significant differences in Project Server architecture between versions. The required operating systems, database servers, and client web browsers that are supported also differ. Plan how to test or rebuild your customizations for the new environment. Planning also provides a good opportunity to consider whether each customization is still needed. For more information, see [Create a plan for current customizations during upgrade to SharePoint 2013](#).
- **Time and patience** - Upgrade planning, execution, and testing will take time and effort, especially if you upgrade to Project Server 2016. For example, if you migrate from Project Server 2007 to Project Server 2016, you first need to migrate to Project Server 2010, check your data, and then do the same thing when you migrate to each successive version. You might want to check with a Microsoft Partner to get estimates of how long it will take and what it will cost.

Migrate to Project Online

If you choose to migrate from Project Server 2007 to Project Online, you can do the following to manually migrate your project plan data:

1. Save your project plans from Project Server 2003 to .mpp format.
2. In Project Professional 2013, Project Professional 2016, or the Project Online Desktop Client, open each .mpp file, and then save and publish it to Project Online.

You can manually create your Microsoft Project Web App (PWA) configuration in Project Online. For example, recreate any needed custom fields or enterprise calendars. Microsoft Partners can also help with this process.

Key resources:

RESOURCE	DESCRIPTION
Get started with Project Online	How to set up and use Project Online
Project Online Service Descriptions	Information about the different Project Online plans that are available to you

Migrate to a newer on-premises version of Project Server

We strongly believe that you get the best value and user experience by migrating to Project Online. But we also understand that some organizations need to keep project data in an on-premises environment. If you choose to keep your project data on-premises, you can migrate your Project Server 2007 environment to Project Server 2010, Project Server 2013, or Project Server 2016.

If you can't migrate to Project Online, we recommend that you migrate to Project Server 2016. Project Server 2016 includes all the features of previous releases of Project Server. It most closely matches the experience available with Project Online, although some features are available only in Project Online.

After each migration, you should check that your data migrated successfully.

NOTE

How do I migrate to Project Server 2016?

Architectural differences between Project Server 2007 and Project Server 2016 prevent a direct migration path. So you have to migrate your Project Server 2007 data to each successive version of Project Server until you reach Project Server 2016.

Follow these steps to Project Server 2016:

1. Migrate from Project Server 2007 to Project Server 2010.
2. Migrate from Project Serve 2010 to Project Server 2013.
3. Migrate from Project Server 2013 to Project Server 2016.

After each migration, make sure that your data migrated successfully.

Step 1: Migrate from Project Server 2007 to Project Server 2010

For a comprehensive description of what you need to do to upgrade from Project Server 2007 to Project Server 2010, see [Upgrade to Project Server 2010](#).

Key resources:

RESOURCE	DESCRIPTION
Project Server 2010 upgrade overview	A high-level view of what you need to do to upgrade from Project Server 2007 to Project Server 2010
Plan to Upgrade to Project Server 2010	Planning considerations when you upgrade from Project Server 2007 to Project Server 2010, including System Requirements

How do I upgrade?

For details, see [Upgrade to Project Server 2010](#). But it's important to understand that there are two distinct

methods you can use to upgrade:

- **Database-attach upgrade:** This method only upgrades the content for your environment, not the configuration settings. It's required if you're upgrading from Office Project Server 2007 deployed on hardware that only supports a 32-bit server operating system. There are two types of database-attach upgrade methods:
 - **Database-attach *full upgrade*** - Migrates the project data stored in the Office Project Server 2007 databases, plus the Microsoft Project Web App site data stored in a SharePoint content database.
 - **Database-attach *core upgrade*** - Migrates only the project data stored in the Project Server databases.
- **In-place upgrade:** The configuration data for the farm and all content on the farm is upgraded on the existing hardware in a fixed order. When you start the upgrade process, setup takes the entire farm offline. The web sites and Microsoft Project Web App sites are unavailable until the upgrade is finished, and then setup restarts the server. After you begin an in-place upgrade, you can't pause the upgrade or roll back to the previous version. It's best to make a mirrored image of your production environment and do the in-place upgrade to this environment, not in your production environment.

Additional resources:

- [SuperFlow for Microsoft Project Server 2010 Upgrade](#)
- [Migration from Project Server 2007 to Project Server 2010](#)
- [Upgrade considerations for Project Web App Web Parts](#)
- [Project Software Development Kit \(SDK\)](#)

Step 2: Migrate to Project Server 2013

After you verify that your data migrated successfully, the next step is to migrate to Project Server 2013.

For a comprehensive description of what you need to do to upgrade from Project Server 2010 to Project Server 2013, see [Upgrade to Project Server 2013](#).

Key resources:

RESOURCE	DESCRIPTION
Overview of the Project Server 2013 upgrade process	Overview of what you need to do to upgrade from Project Server 2010 to Project Server 2013
Plan to upgrade to Project Server 2013	Planning considerations when you upgrade from Project Server 2010 to Project Server 2013, including System Requirements

Things to know about upgrading to this version

[What's new in Project Server 2013 upgrade](#) describes important changes for upgrade for this version. The most notable are:

- There's no in-place upgrade to Project Server 2013. The database-attach method is the only supported method for upgrading from Project Server 2010 to Project Server 2013.
- The upgrade process will not only convert your Project Server 2010 data to Project Server 2013 format but will also consolidate the four Project Server 2010 databases into a single Project Web App database.
- In the 2013 versions, both SharePoint Server and Project Server changed to claims-based authentication.

If you're using classic authentication, you need to consider this factor for your upgrade. For more information, see [Migrate from classic-mode to claims-based authentication in SharePoint 2013](#).

Additional resources:

- [Overview of the upgrade process to Project Server 2013](#)
- [Upgrade your databases and Project Web App site collections \(Project Server 2013\)](#)
- [Microsoft Project Server upgrade process diagram](#)
- [The Great Database Consolidation, Project Server 2010 to 2013 Migration in 8 Easy Steps](#)

Step 3: Migrate to Project Server 2016

After you verify that your data migrated successfully, the next step is to migrate to Project Server 2016.

For a comprehensive description of what you need to do to upgrade from Project Server 2013 to Project Server 2016, see [Upgrade to Project Server 2016](#).

Key resources:

RESOURCE	DESCRIPTION
Overview of the Project Server 2016 upgrade process	Overview of what you need to do to upgrade from Project Server 2013 to Project Server 2016
Plan for upgrade to Project Server 2016	Planning considerations you upgrade from Project Server 2013 to Project Server 2016

Things to know about upgrading to this version

[Things you need to know about Project Server 2016 upgrade](#) tells you some important changes for upgrade for this version, which include:

- When you create your Project Server 2016 environment to which you'll migrate your Project Server 2013 data, the Project Server 2016 installation files are included in SharePoint Server 2016. For more information, see [Deploy Project Server 2016](#).
- Resource plans are deprecated in Project Server 2016. Your Project Server 2013 resource plans will be migrated to Resource Engagements in Project Server 2016 and in Project Online. See [Overview: Resource engagements](#) for more information.

Migrate from Portfolio Server 2007

Project Portfolio Server 2007 was used with Project Server 2007 for portfolio strategy, prioritization, and optimization. No additional versions of Project Portfolio Server were created after this version. However, portfolio management features are available in Project Server 2016 and the Premium version of Project Online. But data from Project Portfolio Server 2007 can't be migrated to either. Data such as business drivers will have to be recreated.

Other resources:

- [Project Online Service Descriptions](#): See the portfolio management features that are included with Project Server 2016 and Project Online Premium.
- [Microsoft Office Project Portfolio Server 2007 migration guide](#).

Related topics

[SharePoint Server 2007 end of support Roadmap](#)

[Resources to help you upgrade from Office 2007 servers and clients](#)

Cloud services roadmap for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

To get the creativity, teamwork, and productivity benefits of Microsoft 365 for enterprise, deploy the cloud services that best fit your organization's needs.

If you have existing server-based deployments for Exchange, SharePoint, or Skype for Business and want to migrate your entire organization to Microsoft 365 for enterprise, see the [client and server software roadmap](#). This roadmap includes Microsoft Office client products, on-premises Office Server products, and Microsoft Windows-based devices.

Deploy

To deploy your cloud services:

- [Get your services ready](#)
- [Migrate your on-premises data to Microsoft 365](#)
- Get your cloud services set up for your users
 - [Exchange Online](#)
 - [SharePoint](#)
 - [Microsoft Teams](#)
 - [Yammer](#)
- [Train your users](#)

Manage

To manage your cloud services:

- [Check your service health](#)
- [Understand your support options](#)
- Administer your cloud services
 - [Exchange Online](#)
 - [SharePoint](#)
 - [Skype for Business](#)
 - [Teams](#)
 - [Yammer](#)
- [Perform performance tuning for your cloud services](#)

How Microsoft does cloud services for Microsoft 365

For information about how Microsoft IT has deployed or is managing Microsoft 365 cloud services:

1. Go to [Microsoft IT Showcase](#).
2. Select **Search content**.
3. Under **Refine results**, select **IT Pro** under **Audience**, and then under **Product**, select a cloud service.

Next step

Start your cloud services implementation. For guidance, see [Configure Microsoft 365 Enterprise services and](#)

applications.

Configure Microsoft 365 Enterprise services and applications

10/28/2022 • 2 minutes to read • [Edit Online](#)

Our [basic set up instructions](#) help you get everyone using your Microsoft 365 services and applications in the shortest time possible. Sometimes getting things configured before everyone starts using them is preferred. For example if you want to configure mail routing, file storage, or sharing policies.

If you want help getting Microsoft 365 set up, use [FastTrack](#) or the [Setup guides for Microsoft 365 and Office 365 services](#).

SERVICES & APPLICATIONS	RESOURCES
Microsoft 365 Suite	- Add your company branding to Microsoft 365 Sign In Page - Add customized help desk info to the Microsoft 365 help pane - Add integration with Azure AD and other applications. - Activate and use mobile device management in Microsoft 365 - Monitor Microsoft 365 connectivity
Email (Exchange Online)	- Use the Exchange migration advisor to get customized setup guidance - Set up Exchange Online Protection
Sites (SharePoint)	- Configure hybrid functionality for SharePoint Server - Use the SharePoint Planning Guide or the SharePoint deployment advisor to plan and configure additional features
IM and online meetings (Teams)	- Microsoft Teams deployment overview - Meetings and conferencing in Microsoft Teams - Plan your Teams voice solution
File storage & sharing (OneDrive and SharePoint)	- Set up Microsoft 365 file storage and sharing: Learn when you should use OneDrive to store files and when you should use SharePoint team sites - Use the OneDrive setup guide to get customized setup guidance
Microsoft 365 applications	- Microsoft 365 administrators should use the Office Deployment Guide to get help planning a Microsoft 365 Apps for enterprise deployment or upgrade. - Power BI for Microsoft 365 admin center - Get started with Project for the web. - Microsoft Intune deployment advisor
Enterprise Social (Yammer)	- Use Yammer with Microsoft 365 - Use the Yammer Enterprise setup guide to get customized setup guidance

Overview of external collaboration options in Microsoft 365

10/28/2022 • 6 minutes to read • [Edit Online](#)

With Microsoft 365, your users can collaborate with people outside your organization in a variety of ways. Users can share files, invite guests to teams, have meetings with external participants, and chat with people from other organizations. This article covers the external collaboration options available and links to the content you need to configure each.

The following table shows the primary ways people from outside your organization can access your Microsoft 365 resources:

ACTIVITY	ACCOUNT TYPE	DEFAULT SETTING
Authenticated file and folder sharing	Guest account	Enabled
Site sharing	Guest account	Enabled
Team sharing	Guest account	Enabled
Shared channel in Teams	Existing Microsoft 365 external account	Disabled
External chat and meetings	Existing Microsoft 365 external account	Enabled
Anonymous meeting join	None	Enabled
Unauthenticated file and folder sharing	None	Enabled

People outside your organization do not have access unless a user in your organization initiates one of these activities. You can disable any of these settings if you don't want to allow that activity in your organization.

Document, site, and team sharing with guest accounts

Sharing documents, sites, and teams with people outside your organization uses *guest accounts*. Guest accounts are a type of account in Azure Active Directory that is managed through [Azure AD B2B collaboration](#). They can be used to share resources in your organization with anyone who has an email address. You can manage guest accounts the same way you manage users in your organization. Guests do not require a license for most features of collaboration.

Guests can only access resources that you specifically share with them.

If the guest has a work or school account in another organization, or a Microsoft account, they can log in with their regular username and password. If they have a different type of account - such as a Gmail account - they can log in by using a one-time passcode that is sent to their email address.

With guests you can:

- Invite them to Microsoft 365 groups, teams, or SharePoint sites where they can collaborate with people in your organization.

- Share a single file or a folder with them which they can view or edit depending on the permissions you give them.

For information about how to plan for collaboration with guests in Microsoft 365, see the following references:

- [Plan external collaboration](#)
- [Set up secure file sharing and collaboration with Microsoft Teams](#)

For information about how to set up Microsoft 365 for collaboration with guests, see the following references:

- [Collaborate with guests on a document](#)
- [Collaborate with guests in a site](#)
- [Collaborate with guests in a team](#)

Shared channels

Shared channels are a type of Teams channel that allows you to share with people outside the team, including people in other Microsoft 365 organizations. While shared channels is turned on by default in Teams, external collaboration with shared channels is disabled by default. External collaboration with shared channels uses [Azure AD B2B direct connect](#) which allows you to add people from other Microsoft 365 organizations to Teams channels without the need for creating a guest account.

Shared channels have a particular advantage over guest accounts in that they do not require external participants to switch orgs in the Teams desktop client or log into your organization. They can remain logged in to their organization and access the channel directly.

Sharing channels with people outside your organization requires that your organization and the external organization both configure an organizational relationship in [Azure AD B2B Direct Connect](#).

For information about how to set up Microsoft 365 for external collaboration with shared channels, see the following references:

- [Plan external collaboration](#)
- [Shared channels in Microsoft Teams](#)
- [Collaborate with external participants in a channel](#)

External chat and meetings

Users in your organization can chat, add users to meetings, and use audio or video conferencing in Teams with users in external Microsoft 365 organizations. By default, users in your organization can communicate in these ways with all other Microsoft 365 domains. People in other organizations can communicate in these ways with your users if they know the user's email address. You can allow or block specific domains or block all domains if you want to disable the feature.

You can also allow users in your organization to communicate with people from outside your organization who are using Teams accounts that are not managed by an organization, as well as Skype for Business (online and on-premises) and Skype users.

Guest accounts are not used as part of external chat and meetings. External participants remain signed in to their organization or to Skype and can communicate directly with people in your organization. They do not have access to your teams or channels.

For information about how to set up Microsoft 365 for external chat and meetings, see the following references:

- [Use guest access and external access to collaborate with people outside your organization](#)
- [Manage external access in Microsoft Teams](#).

Anonymous meeting join

People from outside your organization can join meetings in the following ways:

- If they're logged in to your organization with a guest account, they join meetings as a guest.
- If they're logged in to a different organization with a work or school account, and your organization has enabled external access, they join meetings as an external participant.
- If they're not a guest or external participant, they must join meetings anonymously.

If the anonymous join setting is enabled for your organization, anonymous users can only join a meeting using a meeting link that has been shared with them (such as a link in the meeting invitation). They will be prompted to enter a display name of their choosing when joining the meeting anonymously. Depending on the lobby settings, the anonymous user may be automatically admitted to the meeting, or be added to a lobby where the meeting organizer (or meeting participants with the presenter role) can allow or deny access to the meeting.

It is not possible to verify the identity of anonymous users before, during or after the meeting.

You can control anonymous users' ability to join meetings at the organization level. If it's enabled for the organization, meeting organizers can control anonymous join through meeting policy settings.

For information about configuring anonymous join for meetings, see [Manage meeting settings in Microsoft Teams](#).

Unauthenticated file and folder access

In Microsoft 365, files and folders in Teams, SharePoint, and OneDrive can be shared using unauthenticated - or *Anyone* - links. Anyone links give access to the shared item to anyone who has the link. Anyone links can be shared with others, giving those people access to the file or folder.

People using an Anyone link do not have to authenticate, and their access cannot be audited. File and folder owners can revoke access at any time by deleting the link.

Anyone links can't be used with files in a Teams shared channel site.

For information about working with anonymous file and folder sharing, see the following references:

- [Manage sharing settings](#)
- [Best practices for sharing files and folders with unauthenticated users](#)

Related topics

[Intro to file collaboration in Microsoft 365, powered by SharePoint](#)

[File collaboration in SharePoint with Microsoft 365](#)

[Use guest access and external access to collaborate with people outside your organization](#)

[Limit guest sharing to specific organizations](#)

[Limit organizations where users can have guest accounts](#)

Activate rights management in the admin center

10/28/2022 • 2 minutes to read • [Edit Online](#)

You must activate the Rights Management service (RMS) before you can use the Information Rights Management (IRM) features of Microsoft 365 applications and services. After you activate RMS, your organization can start to protect important documents and emails by using Azure RMS. This information protection solution can protect all file types and integrates with client applications like Excel, Microsoft Word, and others, Exchange Online and SharePoint Online, and servers such as Microsoft Exchange and Microsoft SharePoint.

TIP

If you're not sure whether you need Rights Management, check whether your organization has one or more of [these business problems or requirements](#).

Use these links for more information about RMS:

- To learn more about RMS, see [What is Azure Rights Management](#).
- If you're new to RMS, see [Overview of Azure Rights Management](#).
- For an overview of the deployment steps see the [Azure Rights Management deployment road map](#).
- For instructions about activating RMS for Microsoft 365, see [Activating the protection service from Azure Information Protection](#).

How to check Microsoft 365 service health

10/28/2022 • 7 minutes to read • [Edit Online](#)



The Admin Center is changing. If your experience doesn't match the details in this article, check out <https://aka.ms/aboutM365preview>.

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the **Service health** page in the [Microsoft 365 admin center](#). If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

If you are unable to sign in to the admin center, you can use the [service status page](#) to check for known issues preventing you from logging into your tenant. Also sign up to follow us at [@MSFT365status](#) on Twitter to see information on certain events.

How to check service health

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>, and sign in with an admin account.

NOTE

People who are assigned the global admin or service support admin role can view service health. To allow Exchange, SharePoint, and Skype for Business admins to view service health, they must also be assigned the Service admin role. For more information about roles that can view service health, see [About admin roles](#).

2. To view service health, in the left-hand navigation of the admin center, go to **Health > Service health**, or select the **Service health** card on the **Home dashboard**. The dashboard card indicates whether there is an active service issue and links to the detailed **Service health** page.
3. On the **Service health** page, the health state of each cloud service is shown in a table format.

Service health

[All services](#) [Incidents](#) [Advisories](#) [History](#) [Reported issues](#)

View the health status of all services that are available with your current subscriptions.

[Report an issue](#) [Preferences](#)

Service	Health	Status	Updated
Microsoft 365 suite	2 advisories		
Admins may see delays with license reports in the admin center	Advisory	Service degradation	August 8, 2021 8:37 PM
Admins see some users' Outlook Desktop activity isn't shown in usage reports	Advisory	Service degradation	August 2, 2021 11:39 PM
SharePoint Online	1 advisory		
Azure Information Protection	Healthy		
Cloud App Security	Healthy		
Dynamics 365 Apps	Healthy		

The **All services** tab (the default view) shows all services, their current health state, and any active incidents or advisories. An icon and status in the **Health** column indicate the state of each service.

If there is an active incident or advisory for a service they will be listed directly under the service name in a nested table. You can collapse the nested table to hide the incidents or advisories in this view by clicking on the chevron icon to the left of the service name.

To filter your view to only show all the active incidents, select the **Incidents** tab at the top of the page. Selecting the **Advisories** tab will only show all the active advisories posted.

The **History** tab shows all incidents and advisories that have been resolved within the last seven or 30 days.

If you're experiencing an issue with a Microsoft 365 service and you don't see it listed on the **Service health** page, tell us about it by selecting **Report an issue**, and completing the short form. We'll look at related data and reports from other organizations to see how widespread the issue is, and if it originated with our service. If it did, we'll add it as a new incident or advisory on the **Service health** page, where you can track its resolution. The **Reported Issues** page will show all issues your tenant has reported from this form and the status.

To customize your view of which services show up on the dashboard, select **Preferences > Custom view**, and clear the checkboxes for the services you want to filter out of your Service health dashboard view. Make sure that the checkbox is selected for each service that you want to monitor.

To sign up for email notifications of new incidents that affect your tenant and status changes for an active incident, select **Preferences > Email**, click **Send me service health notifications in email**, and then specify:

- Up to two email addresses.
- Whether you want notifications for incidents or advisories
- The services for which you want notification

You can also subscribe to email notifications for individual events instead of every event for a service. To do so, select the active issue you want to receive email notification updates for, select **Manage notifications for this issue**, and then specify:

- Up to two email addresses.

NOTE

Each admin can have their Preferences set and the above limit of two email address is per admin account.

TIP

You can also use the [Microsoft 365 Admin app](#) on your mobile device to view Service health, which is a great way to stay current with push notifications.

View details of posted service health

On the **All services** view, select the issue title to see the issue detail page, which shows more information about the issue, including a feed of all the messages posted while we work on a solution.

Service health

May 15, 2020 11:39 AM

All services

Incidents

Advisories

History

Reported issues

An advisory is a service issue that is typically limited in scope or impact.

Report an issue

Preferences

3 items

Search

Exchange Online

Title	Service	ID	Status	Start time ↓	Last updated
Any user with end-user spam notification (ESN) policies ...	Exchange Online	EX213379	Extended recovery	May 15, 2020 11:00 AM	May 15, 2020 11:19 AM
Many users will see searches failing in the Outlook desk...	Exchange Online	EX212460	Restoring service	May 8, 2020 6:29 PM	May 13, 2020 4:48 PM
All admins seeing extra option when releasing quarantin...	Exchange Online	EX211743	Service degradation	April 6, 2020 12:00 PM	May 8, 2020 1:19 PM

The advisory or incident summary provides the following information:

- **Title** - A summary of the problem.
- **ID** - A numeric identifier for the problem.
- **Service** - The name of the affected service.
- **Last updated** - The last time that the service health message was updated.
- **Estimated Start time** - The estimated time when the issue started.
- **Status** - How this problem affects the service.
- **User Impact** - A brief description of the impact this issue has on the end user.
- **All Updates** - We post frequent messages to let you know the progress that we're making in applying a solution.

Duplicate calendar events

EX192143, Exchange Online, Last updated: October 8, 2019 4:17 PM

Start time: July 14, 2019 5:00 PM

Status

Service degradation

User impact

Users may see duplicate calendar events on other account calendars when using Outlook on the web.

[Are you experiencing this issue?](#)

[Is this post helpful?](#)

Latest message [View history](#)

Title: Duplicate calendar events

User Impact: Users may see duplicate calendar events on other account calendars when using Outlook on the web.

More info: While we're focused on remediation, users may utilize the Outlook desktop client to view other account calendars without duplicate events. Furthermore, this issue is cosmetic in nature and shouldn't affect the functionality of Outlook on the web.

Additionally, this issue specifically occurs when viewing other users' shared calendars in Agenda View, My Day panel, and other specific calendar views. The calendar events will appear to be duplicated, however changes to any of the events will properly propagate to the original event and their respective duplicates.

We'd like to get your feedback on the workaround we provided. From a non-mobile device, please rate this post and submit it in the textbox.

Current status: We've begun the deployment of the fix to the affected environments and it has reached 10 percent saturation. We expect the fix to be fully saturated by Thursday, October 10, 2019, 6:00 PM (10/11/2019, 1:00 AM UTC)

.

Scope of impact: This can potentially impact any of your users that are viewing other users' calendars using Outlook on the web with specific layouts.

Start time: Sunday, July 14, 2019, 5:00 PM (7/15/2019, 12:00 AM UTC)

Root cause: A code issue within Outlook on the web calendars is resulting in a caching problem when Outlook on the web fetches other account's calendars, causing duplicate calendar events.

Next update by: Friday, October 11, 2019, 6:00 PM (10/12/2019, 1:00 AM UTC)

Translate service health details

We use machine translation to automatically display messages in your preferred language. Read [Language translation for Service health dashboard](#) for more information on how to set your language.

Definitions

Most of the time, services will appear as healthy with no further information. When a service is having a problem, the issue is identified as either an advisory or an incident and shows a current status.

TIP

Planned maintenance events aren't shown in service health. You can track planned maintenance events by staying up to date with the **Message center**. Filter to messages categorized as Plan for change to find out when the change is going to happen, its effect, and how to prepare for it. See [Message center in Microsoft 365](#) for more details.

Incidents and advisories

ICON	DESCRIPTION
	If a service has an advisory shown, we are aware of a problem that is affecting some users, but the service is still available. In an advisory, there is often a workaround to the problem and the problem may be intermittent or is limited in scope and user impact.
	If a service has an active incident shown, it's a critical issue and the service or a major function of the service is unavailable. For example, users may be unable to send and receive email or unable to sign-in. Incidents will have noticeable impact to users. When there is an incident in progress, we will provide updates regarding the investigation, mitigation efforts, and confirmation of resolution in the Service health dashboard.

Status definitions

STATUS	DEFINITION
Investigating	We're aware of a potential issue and are gathering more information about what's going on and the scope of impact.
Service degradation	We've confirmed that there is an issue that may affect use of a service or feature. You might see this status if a service is performing more slowly than usual, there are intermittent interruptions, or if a feature isn't working, for example.
Service interruption	You'll see this status if we determine that an issue affects the ability for users to access the service. In this case, the issue is significant and can be reproduced consistently.
Restoring service	The cause of the issue has been identified, we know what corrective action to take, and are in the process of bringing the service back to a healthy state.
Extended recovery	This status indicates that corrective action is in progress to restore service to most users but will take some time to reach all the affected systems. You might also see this status if we've made a temporary fix to reduce impact while we wait to apply a permanent fix.
Investigation suspended	If our detailed investigation of a potential issue results in a request for additional information from customers to allow us to investigate further, you'll see this status. If we need you to act, we'll let you know what data or logs we need.

STATUS	DEFINITION
Service restored	We've confirmed that corrective action has resolved the underlying problem and the service has been restored to a healthy state. To find out what went wrong, view the issue details.
False positive	After a detailed investigation, we've confirmed the service is healthy and operating as designed. No impact to the service was observed or the cause of the incident originated outside of the service. Incidents and advisories with this status appear in the history view until they expire (after the period of time stated in the final post for that event).
Post-incident report published	We've published a Post Incident Report for a specific issue that includes root cause information and next steps to ensure a similar issue doesn't reoccur.

Message Post Types

TYPE	DEFINITION
Quick Update	Short and frequent incremental updates for broadly impacting incidents, available to all customers.
Additional Details	These additional posts will provide richer technical and resolution details to offer deeper visibility into the handling of incidents. This is available for tenants that meet the same requirements outlined for Exchange Online monitoring ,

History

Service health lets you look at your current health status and view the history of any service advisories and incidents that have affected your tenant in the past 30 days. To view the past health of all services, select **History** view.

For more information about our commitment to uptime, see [Transparent operations from Microsoft 365](#).

Related topics

- [Activity Reports in the Microsoft 365 admin center](#)
- [Message center Preferences](#)
- [How to check Windows release health on admin center](#)

Get support for Microsoft 365 for business

10/28/2022 • 9 minutes to read • [Edit Online](#)

Check out [Microsoft 365 small business help](#) on YouTube.

Watch: Get help or support

Check out this video and others on our [YouTube channel](#).

Need to speak to someone right away? Admins, have your account details ready when you call Support.

IMPORTANT

You must be an admin for a business subscription to use these support methods. If you're not a business admin, please use [this support page](#).

Start by [checking the current health of your services](#). You can view detailed information about current and past issues on the [Service health dashboard](#). If you're experiencing an issue that isn't listed, you can get support in one of the following ways:

Online support

Save time by starting your service request online. We'll help you find a solution or connect you to technical support.

1. Go to the admin center at <https://admin.microsoft.com>. If you get a message that says you don't have permission to access this page or perform this action, you aren't an admin. For more information, see [Who has admin permissions in my business?](#)
2. On the bottom right side of the page, select **Help & support**.
3. Type a question or keyword into the text box. If you get a drop-down list, select the one closest to your question, or continue typing your question, then press **Enter**.
4. If the results don't help, at the bottom, select **Contact Support**.
5. Enter a description of your issue, confirm your contact number and email address, select your preferred contact method, and then select **Contact me**. The expected wait time is indicated in the **Contact support** pane.

NOTE

If you bought your subscription through a partner, you first see the contact information for that partner. Alternatively, select **New Microsoft service request** at the bottom of the pane.

Phone support

In most countries or regions, billing support for Microsoft 365 for business products and services is provided in English from 9 AM-5 PM, Monday through Friday. Local language support varies by country or region.

Technical support is provided in English 24 hours a day, 7 days a week, and in some cases, in local languages as noted.

[Find support phone numbers by country or region](#)

Admins, have your account details ready when you call.

NOTE

To better protect your organization, we added a PIN-based verification step to our existing phone-based verification process. If you contact us from a number that isn't registered with your organization profile, the Microsoft support representative sends a verification code to the registered email or phone number in your Microsoft 365 admin center profile. You must provide this code to the support representative to grant them access to your organization's account.

Small business support with Business Assist

Get the most out of your subscription with expert advice from small business specialists.

Business Assist for Microsoft 365 is designed for small businesses to give you and your employees around-the-clock access to small business specialists as you grow your business, from onboarding to everyday use. To learn more, see [Business Assist](#).

With every subscription of Office 365 operated by 21Vianet, 21Vianet support provides technical, pre-sales, billing and subscription support. Support is available both online through the Office 365 operated by 21Vianet portal, and by telephone for both paid and trial subscriptions.

Authorized administrators can use the Office 365 operated by 21Vianet portal to submit service requests online and access support telephone numbers. For instructions, see [Contact support](#).

The Office 365 operated by 21Vianet technical support team troubleshoots only those issues that are related to Office 365 operated by 21Vianet. Issues that originate in customer networks fall outside of the Office 365 support boundaries, and in these cases, customers must work with their networking team for assistance.

Community and self-service support options

Self-service support is available for all Office 365 operated by 21Vianet users, and includes troubleshooting tools and videos, help articles and videos, as well as forums and wikis in the [Office 365 community](#). For more self-help resources, see [Learn about Office 365 operated by 21Vianet](#).

Pre-sales support

Pre-sales support for Office 365 operated by 21Vianet provides assistance on subscription features and benefits, plan comparisons, pricing and licensing, and helps to identify the right solution to meet your business needs. In addition, pre-sales support can help you find a Partner, and purchase and sign up for a trial. You can call during local business hours, Monday through Friday. Pre-sales support can be accessed using the same phone number as with technical support. For instructions, see [Contact support](#).

Billing and subscription management support

Assistance for billing and subscription management issues is available online or by telephone during China business hours (Beijing Time), Monday through Friday. Billing and subscription management support can be accessed using the same phone number and online service request process as with technical support. The support telephone number can be found on the Office 365 operated by 21Vianet portal. For instructions, see [Contact support](#).

Here are some examples of billing and subscription management issues:

- Signing up for a trial or purchasing a subscription
- Converting from a trial subscription to a paid subscription
- Understanding the bill
- Renewing a subscription
- Adding or removing licenses
- Canceling a paid subscription

Technical support

Technical support for Office 365 operated by 21Vianet subscriptions provides assistance with basic installation, setup, and general technical usage. Some examples of these issues are listed in the following table.

SUPPORT CATEGORY	EXAMPLES
Installation and setup	Exchange Online • Office 365 mailbox migration • Recipient configuration (mailbox permissions, configuring mail forwarding, configuring shared mailbox) • Autodiscover configuration SharePoint Online • Permissions and user groups • Configuration of external users Skype for Business Online • Installation and creating contacts Microsoft 365 Apps for enterprise • Installation and setup
Configuration	Service configuration issues • Single sign-on (SSO) • Active Directory synchronization

NOTE

You can learn how to contact technical support here: [Contact support](#). Technical support does not include troubleshooting third-party services or add-ins. Learn about finding answers from other customers in the [Community](#).

Technical support case handling

21Vianet assigns a severity level to a case when it is opened, based on an assessment of the issue type and customer impact. Examples of issue types and severity levels are shown in the following table.

SEVERITY LEVEL	OPERATIONS AND SUPPORT DESCRIPTION	EXAMPLES
----------------	------------------------------------	----------

SEVERITY LEVEL	OPERATIONS AND SUPPORT DESCRIPTION	EXAMPLES
Sev A (Critical)	One or more services aren't accessible or are unusable. Production, operations, or deployment deadlines are severely affected, or there will be a severe impact on production or profitability. Multiple users or services are affected.	- Widespread problems sending or receiving mail. - SharePoint site down. - All users can't send instant messages, join or schedule Skype for Business Meetings, or make Skype for Business calls.
Sev B (High)	The service is usable but in an impaired fashion. The situation has moderate business impact and can be dealt with during business hours. A single user, customer, or service is partially affected.	- Send button in Outlook is garbled. - Setting is impossible from EAC (Exchange admin center) but possible in Exchange Online PowerShell.
Sev C (Non-critical)	The situation has minimal business impact. The issue is important but does not have a significant current service or productivity impact for the customer. A single user is experiencing partial disruption, but an acceptable workaround exists.	- How to set user password that never expires. - User can't delete contact information in Exchange Online.

Technical support initial response times

Initial response time is based on the severity levels described above. 21Vianet customer service team follow up with investigation and customer communication in reasonable rhythm according to severity levels. 21Vianet also expect customer to collaborate at reasonable level accordingly.

SECURITY LEVEL ¹	21VIANET CUSTOMER SUPPORT TEAM INITIAL RESPONSE	CUSTOMER RESPONSIBILITY
Sev A ² (Critical)	Initial Response: 1 hour or less. Follow up: continues effort until problem resolution.	Provide solid business impact statement (see the severity A description and examples above); Allocate resource to ensure continues collaboration with 21Vianet customer support agent for the joint investigation and necessary communication; Provide accurate contact information and ensure reliable communication throughout the service request lifecycle.
Sev B (High)	Initial Response: 1 business day or less.	Provide accurate contact information and ensure reliable communication throughout the service request lifecycle.
Sev C (Medium)	Initial Response: 3 business day or less.	Provide accurate contact information and ensure reliable communication throughout the service request lifecycle.

¹ If the customer cannot provide required resource or make response for collaboration with 21Vianet customer support agent investigation in reasonable time, 21Vianet support team may lower down the severity level of a service request.

² Severity A is only available to customers who had signed an advanced online service agreement with 21Vianet through a sales account manager. Severity A is available only for technical support. For billing and subscription management support, the highest severity level is B.

Technical support working hours

Severity A: 24*7 continuous service

Severity B/C: 9:00 ~24:00 (Beijing Time) a day, 365 days.

Contact support

NOTE

Assisted support options are for admins of Office 365 subscribed organizations only. If you use Office 365 but you're not an admin, you can still get support in the community forums, or by contacting your admin.

Open an online request

Save time by starting your service request online. Go to the [Microsoft 365 admin center](#), choose **Support > New service request**.

Call support

Call support. If you encounter any problem with online request, phone support is available at (86) 400-089-0365.

Shared support responsibilities

21Vianet understands that receiving timely technical support from qualified professionals is a key aspect of cloud services. Equally important is the critical role that the customer's IT department plays in the support of its users.

Administrator roles and responsibilities

People with administrator roles are the only ones in the customer's organization authorized to access the Admin section of the Office 365 operated by 21Vianet portal and to communicate directly with 21Vianet about Office 365 service requests.

With Office 365 you can designate several types of administrators who serve different functions. This service description uses the generic title administrator to refer to all categories of administrators. For more information about the types of administrator roles, see [Assign admin roles in Microsoft 365 for business](#).

The administrator is:

- Responsible for service administration and account maintenance.
- The primary contact that sets up and supports each service user.
- Authorized to submit service requests to 21Vianet.

The administrator's role is to:

- Provide user account setup and configuration to allow users access to the services.
- Address client connectivity, client software, and mobility installation issues.
- Address service availability issues within the customer's organizational span of control.
- Use self-service support resources to resolve support issues.

The administrator is expected to provide initial assistance for the customer's users. However, if the administrator is unable to resolve issues with the help of self-service support resources, he or she should [Contact support](#).

21Vianet support role

21Vianet's support role is to:

- Troubleshoot and provide technical guidance for customer issues and escalations.
- Gather and validate information related to specific service requests.
- Provide issue coordination and resolution management.
- Maintain communication with the administrators to help ensure that issues are addressed on an ongoing basis.
- Provide assistance with licensing, invoicing, and subscription inquiries.
- Provide assistance with purchasing and trial inquiries.
- Continually gather customer feedback on how to improve the service through surveys.

Feature availability

To view feature availability across Office 365 plans, see [Office 365 Service Description](#).

Follow us on WeChat

Scan this QR code to follow us on WeChat and get the latest updates for Office 365 operated by 21Vianet.



Related content

[Find docs and training](#) (link page)

[Employee quick setup](#) (article)

[Overview of Microsoft 365 Business Premium setup](#) (video)

Tune Microsoft 365 performance

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article links to training courses, blogs, articles, and other resources that tell you how to improve performance of Microsoft 365.

This article is part of the [Network planning and performance tuning for Microsoft 365](#) project.

Articles about fine-tuning Microsoft 365 and Office 365 performance

Take a look at the [top 10 tips for optimizing and troubleshooting your Office 365 network connectivity](#) by Paul Collinge.

For information about using network address translation with Microsoft 365, see [NAT support with Microsoft 365](#).

Office 365 performance tuning using baselines and performance history

10/28/2022 • 24 minutes to read • [Edit Online](#)

There are some simple ways to check the connection performance between Office 365 and your business that will let you establish a rough baseline of your connectivity. Knowing the performance history of your client computer connections can help you detect emerging issues early, identify, and predict problems.

If you're not used to working on performance issues, this article is designed to help you consider some common questions. How do you know the problem you're seeing is a performance issue and not an Office 365 service incident? How can you plan for good performance, long term? How can you keep an eye on performance? If your team or clients are seeing slow performance while using Office 365, and you wonder about any of these questions, read on.

IMPORTANT

Have a performance issue between your client and Office 365 right now? Follow the steps outlined in the [Performance troubleshooting plan for Office 365](#).

Something you should know about Office 365 performance

Office 365 lives inside a high-capacity, dedicated Microsoft network that is monitored by automation and real people. Part of maintaining the Office 365 cloud is performance tuning and streamlining where possible. Since clients of the Office 365 cloud have to connect across the Internet, there's ongoing effort to fine-tune the performance across Office 365 services too.

Performance improvements never really stop in the cloud, so neither does experience with keeping the cloud healthy and quick. Should you have a performance issue connecting from your location to Office 365, it's best not to start with or wait on a Support case. Instead, you should begin investigating the problem from 'the inside out'. That is, start inside of your network, and work your way out to Office 365. Before you open a case with Support, you can gather data and take actions that will explore, and may resolve, the problem.

IMPORTANT

Be aware of capacity planning and limits in Office 365. That information will put you ahead of the curve when trying to resolve a performance issue. Here's a link to the [Microsoft 365 and Office 365 service descriptions](#). This is a central hub, and all the services offered by Office 365 have a link that goes to their own Service Descriptions from here. That means, should you need to see the standard limits for SharePoint Online, for example, you would click [SharePoint Online Service Description](#) and locate its [SharePoint Online Limits section](#).

Make sure you go into your troubleshooting with the understanding that performance is a sliding scale. It's not about achieving an idealized value and maintaining it permanently. Occasional high-bandwidth tasks like on-boarding a large number of users, or doing large data migrations will be stressful, so *plan* for performance impacts then. You should have a rough idea of your performance targets, but many variables play into performance, so performance varies.

Performance troubleshooting isn't about meeting specific goals and maintaining those numbers indefinitely, it's about improving existing activities, given all the variables.

Okay, what does a performance problem look like?

First, you need to make sure that what you are experiencing is indeed a performance issue and not a service incident. A performance problem is different from a service incident in Office 365. Here's how to tell them apart.

Service Incidents happen when the Office 365 service itself is having issues. You may see red or yellow icons under **Current health** in the Microsoft 365 admin center. You may notice performance on client computers connecting to Office 365 is slow. For example, if Current health reports a red icon and you see **Investigating** beside Exchange, you might then also get calls from people in your organization who complain that client mailboxes using Exchange Online are slow. In that case, it's reasonable to assume that your Exchange Online performance was a victim of Service issues.

Current health

Exchange	Service restored ▼
Identity Service	No issues
Lync	No issues
Office 365 Portal	No issues
Office Subscription	No issues
SharePoint	No issues

[View details and history](#)

At this point, you, the Office 365 admin, should check **Current health** and then **View details and history**, often, to keep up to date on maintenance on the system. The **Current health** dashboard was made to update you about changes to, and problems in, the service. The notes and explanations written to health history, admin to admin, are there to help you gauge, and to keep you posted about ongoing work.

The screenshot shows the Office 365 Admin Center interface. At the top is a blue navigation bar with 'Office 365' on the left and links to Outlook, Calendar, People, Newsfeed, OneDrive, Sites, Tasks, and Admin on the right. Below the navigation bar is a breadcrumb trail 'exchange online'. A table with four columns: INCIDENT, DATE AND TIME, STATUS, and DETAILS, is displayed. The 'INCIDENT' column contains a blue circular icon with a white arrow. The 'DETAILS' column contains the following text: 'Final Status: Engineers have completed deployment of the fix which restored service degradation caused by the EAC access issues.', 'User Experience: There was no end-user impact.', and 'Customer Impact: Customer impact appears to have been limited. Affected administrators were unable to view and select some menu items within Exchange Admin Center (EAC). Affected features may have included Role Based Access Control (RBAC), organization sharing, and retention policy. As a workaround, administrators could have executed commands via Powershell.'

A performance issue isn't a service incident, even though incidents can cause slow performance. A performance issue looks like this:

- A performance issue occurs no matter what the admin center **Current health** is reporting for the service.
- A behavior that used to flow takes a long time to complete or never completes.
- You can replicate the problem too, or know it will happen if you do the right series of steps.
- If the problem is intermittent, there can still be a pattern. For example, you know that by 10:00 AM you'll have calls from users who can't always access Office 365. The calls will end around noon.

This list probably sounds familiar; maybe too familiar. Once you're aware it's a performance problem, the

question becomes, "What do you do next?" The rest of this article helps you determine exactly that.

How to define and test the performance problem

Performance issues often emerge over time, so it can be challenging to define the actual problem. Create a good problem statement with a good idea of issue context, and then you need to repeatable testing steps. Here are some examples of problems statements that don't provide enough information:

- Switching from my Inbox to my Calendar used to be something I didn't notice, and now it's a coffee-break. Can you make it act like it used to?
- Uploading my files to SharePoint Online is taking forever. Why is it slow in the afternoon, but any other time, it's fast? Can't it just be fast?

There are several large challenges posed by the problem statements above. Specifically, too many ambiguities to deal with. For example:

- It's unclear how switching between Inbox and Calendar used to act on the laptop.
- When the user says, "Can't it just be fast", what's "fast"?
- How long is "forever"? Is that several seconds? Or many minutes? Or could the user take lunch and the action would finish up 10 minutes after they got back?

The admin and troubleshooter can't be aware of the *details* of the problem from general statements like these. For example, they don't know when the problem started happening. The troubleshooter might not know the user works from home and only ever sees slow switching while on their home network. Or that the user runs other RAM intensive applications on the local client. Admins may not know the user is running an older operating system or hasn't run recent updates.

When users report a performance problem, there's much information to collect. Getting and recording information is called scoping the issue. Here is a basic scoping list you can use to collect information about performance issues. This list is not exhaustive, but it's a place to start:

- On what date did the issue happen, and around what time of day or night?
- What kind of client computer were you using, and how does it connect to the business network (VPN, Wired, Wireless)?
- Were you working remotely or were you in the office?
- Did you try the same actions on another computer and see the same behavior?
- Walk through the steps that are giving you the trouble so that you can write the actions you take down.
- How slow in seconds or minutes is the performance?
- Where in the world are you located?

Some of these questions are more obvious than others. Most everyone will understand a troubleshooter needs the exact steps to reproduce the issue. After all, how else can you record what's wrong, and how else can you test if the issue is fixed? Less obvious are things like "What date and time did you see the issue?", and "Where in the world are you located?", information that can be used in tandem. Depending on when the user was working, a few hours of time difference may mean maintenance is already underway on parts of your company's network. For instance, your company has a hybrid implementation, like a hybrid SharePoint Search, which can query search indexes in both SharePoint Online and an On-premises SharePoint Server 2013 instance, updates may be underway in the on-premises farm. If your company is all in the cloud, system maintenance may include adding or removing network hardware, rolling out updates that are company-wide, or making changes to DNS, or other core infrastructure.

When you're troubleshooting a performance problem, it's a bit like a crime scene, you need to be precise and observant to draw any conclusions from the evidence. In order to do this, you must get a good problem statement by gathering evidence. It should include the computer's context, the user's context, when the problem began, and the exact steps that exposed the performance issue. This problem statement should be, and stay, the topmost page in your notes. By walking through the problem statement again after you work on the resolution, you are taking the steps to test and prove whether the actions you take have resolved the issue. This is critical to knowing when your work, there, is done.

Do you know how performance used to look when it was good?

If you're unlucky, nobody knows. Nobody had numbers. That means nobody can answer the simple question "About how many seconds did it used to take to bring up an Inbox in Office 365?", or "How long did it used to take when the Executives had a Lync Online meeting?", which is a common scenario for many companies.

What's missing here is a performance baseline?

Baselines give you a context for your performance. You should take a baseline occasionally to frequently, depending on the needs of your company. If you are a larger company, your Operations team may take baselines for your on-premises environment already. For example, if you patch all the Exchange servers on the first Monday of the month, and all your SharePoint servers on the third Monday, your Operations team probably has a list of tasks and scenarios it runs post-patching, to prove that critical functions are operational. For example, opening the Inbox, clicking Send/Receive, and making sure the folders update, or, in SharePoint, browsing the main page of the site, going into the enterprise Search page, and doing a search that returns results.

If your applications are in Office 365, some of the most fundamental baselines you can take measure the time (in milliseconds) from a client computer inside your network, to an egress point, or the point where you leave your network and go out to Office 365. Here are some helpful baselines that you can investigate and record:

- Identify the devices between your client computer and your egress point, for example, your proxy server.
 - You have to know your devices so that you have context (IP addresses, type of device, et cetera) for performance problems that arise.
 - Proxy servers are common egress points, so you can check your web browser to see what proxy server it is set to use, if any.
 - There are third-party tools that can discover and map your network, but the safest way to know your devices is to ask a member of your network team.
- Identify your Internet service provider (ISP), write down their contact information, and ask how many circuits how much bandwidth you have.
- Inside your company, identify resources for the devices between your client and the egress point, or identify an emergency contact to talk to about networking issues.

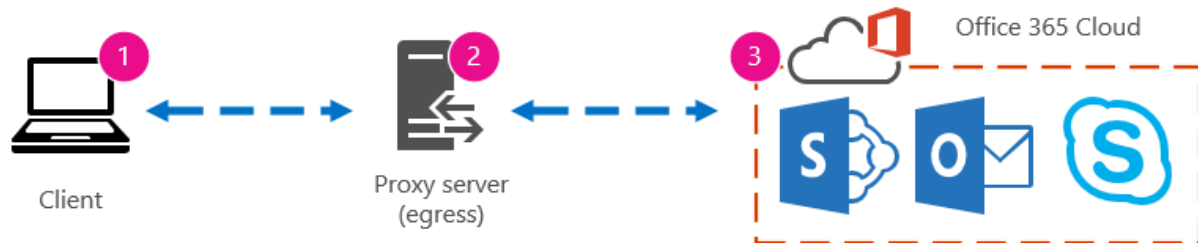
Here are some baselines that simple testing with tools can calculate for you:

- Time from your client computer to your egress point in milliseconds
- Time from your egress point to Office 365 in milliseconds
- Location in the world of the server that resolves the URLs for Office 365 when you browse
- The speed of your ISP's DNS resolution in milliseconds, inconsistencies in packet arrival (network jitter), upload, and download times in milliseconds

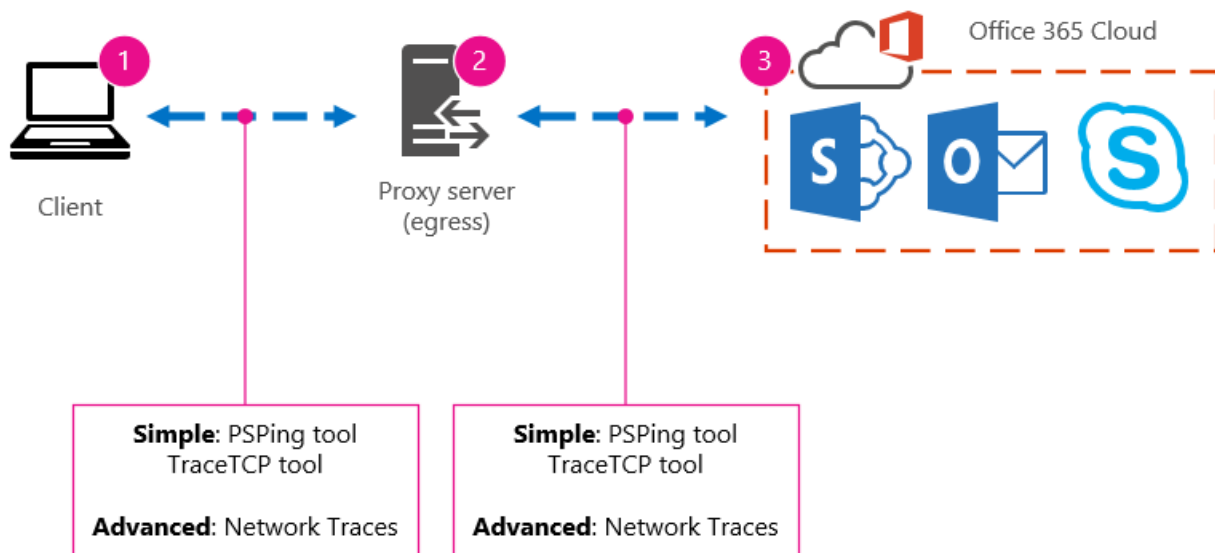
If you're unfamiliar with how to carry out these steps, we'll go into more detail in this article.

What is a baseline?

You'll know the impact when it goes bad, but if you don't know your historical performance data, it's not possible to have a context for how bad it may have become, and when. So without a baseline, you're missing the key clue to solve the puzzle: the picture on the puzzle box. In performance troubleshooting, you need a point of *comparison*. Simple performance baselines aren't difficult to take. Your Operations team can be tasked with carrying these out on a schedule. For example, let's say your connection looks like this:

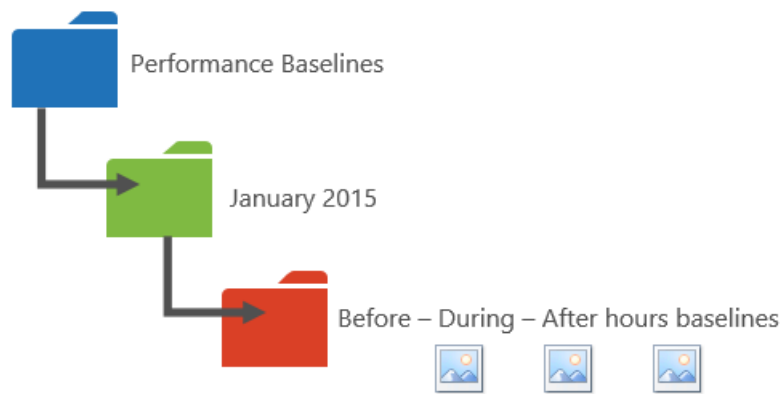


That means you've checked with your network team and found out that you leave your company for the Internet through a proxy server, and that proxy handles all the requests your client computer sends to the cloud. In this case, you should draw a simplified version of your connection that lists all the intervening devices. Now, insert tools that you can use to test the performance between the client, the egress point (where you leave your network for the Internet), and the Office 365 cloud.



The options are listed as **Simple** and **Advanced** because of the amount of expertise you need in order to find the performance data. A network trace will take much time, compared to running command-line tools like PsPing and TraceTCP. These two command-line tools were chosen because they don't use ICMP packets, which will be blocked by Office 365, and because they give the time in milliseconds that it takes to leave the client computer, or proxy server (if you have access) and arrive at Office 365. Each individual hop from one computer to another will end up with a time value, and that's great for baselines! Just as importantly, these command-line tools allow you to add a port number onto the command, this is useful because Office 365 communicates over port 443, which is the port used by Secure Sockets Layer and Transport Layer Security (SSL and TLS). However, other third-party tools may be better solutions for your situation. Microsoft doesn't support all of these tools, so if, for some reason, you can't get PsPing and TraceTCP working, move on to a network trace with a tool like Netmon.

You can take a baseline before business hours, again during heavy use, and then again after hours. This means you may have a folder structure that looks a bit like this in the end:



You should also pick a naming convention your files. Here are some examples:

- Feb_09_2015_9amPST_PerfBaseline_Netmon_ClientToEgress_Normal
- Jan_10_2015_3pmCST_PerfBaseline_PsPing_ClientToO365_bypassProxy_SLOW
- Feb_08_2015_2pmEST_PerfBaseline_BADPerf
- Feb_08_2015_8-30amEST_PerfBaseline_GoodPerf

There are lots of different ways to do this, but using the format **<dateTime> <what's happening in the test>** is a good place to start. Being diligent about this will help a lot when you are trying to troubleshoot issues later. Later, you'll be able to say "I took two traces on February 8, one showed good performance and one showed bad, so we can compare them". This is helpful for troubleshooting.

You need to have an organized way to keep your historical baselines. In this example, the simple methods produced three command-line outputs and the results were collected as screenshots, but you may have network capture files instead. Use the method that works best for you. Store your historical baselines and refer to them at points where you notice changes in the behavior of online services.

Why collect performance data during a pilot?

There is no better time to start making baselines than during a pilot of the Office 365 service. Your office may have thousands of users, hundreds of thousands, or it may have five, but even with a few users, you can perform tests to measure fluctuations in performance. In the case of a large company, a representative sample of several hundred users piloting Office 365 can be projected outward to several thousands so you know where issues might arise before they happen.

In the case of a small company, where on-boarding means that all users go to the service at the same time and there is no pilot, keep performance measures so that you have data to show to anyone who may have to troubleshoot a badly performing operation. For example, if you notice that all of a sudden you can walk around your building in the time it takes to upload a medium-sized graphic where it used to happen quickly.

How to collect baselines

For all troubleshooting plans you need to identify these things at a minimum:

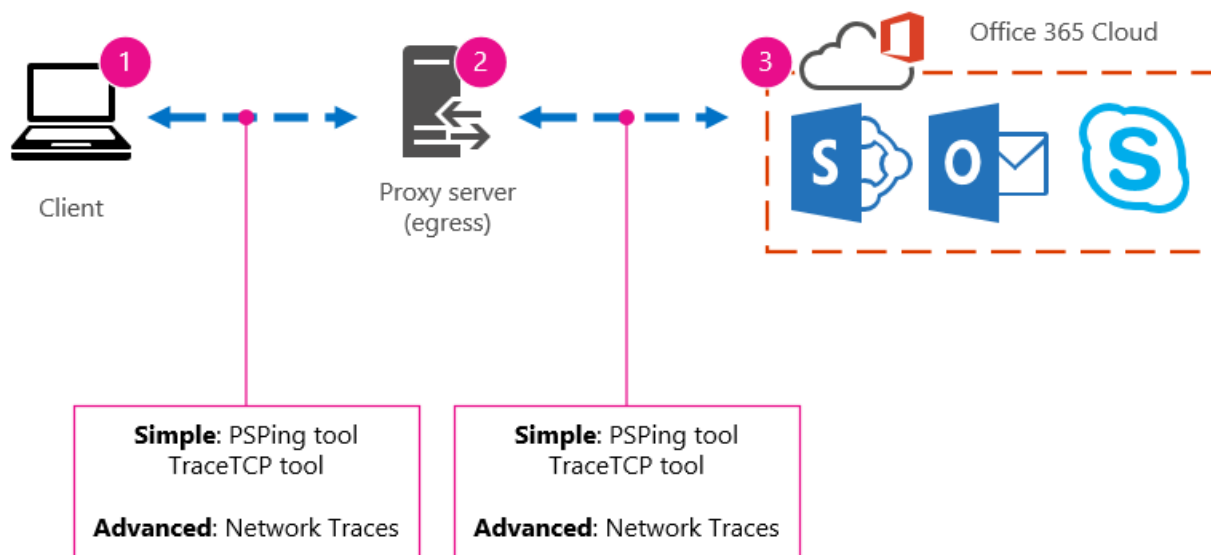
- The client computer you're using (the type of computer or device, an IP address, and the actions that caused the issue)
- Where the client computer is located in the world (for example, whether this user is on a VPN to the network, working remotely, or on the company intranet)
- The egress point the client computer uses from your network (the point at which traffic leaves your business for an ISP or the Internet)

You can find out the layout of your network from the network administrator. If you're on a small network, take a look at the devices connecting you to the Internet, and call your ISP if you have questions about the layout. Create a graphic of the final layout for your reference.

This section is broken into simple command-line tools and methods, and more advanced tools options. We'll cover simple methods first. But if you've got a performance problem right now, you should jump to advanced methods and try out the sample performance-troubleshooting action plan.

Simple methods

The objective of these simple methods is to learn to take, understand, and properly store simple performance baselines over time so that you are informed about Office 365 performance. Here's the simple diagram for simple, as you've seen before:



NOTE

TraceTCP is included in this screen shot because it's a useful tool for showing, in milliseconds, how long a request takes to process, and how many network hops, or connections from one computer to the next, that the request takes to reach a destination. TraceTCP can also give the names of servers used during hops, which can be useful to a Microsoft Office 365 troubleshooter in Support. > TraceTCP commands can be very simple, such as: >

```
tracetcp.exe outlook.office365.com:443
```

> Remember to include the port number in the command! > [TraceTCP](#) is a free download, but relies on Wincap. Wincap is a tool that is also used and installed by Netmon. We also use Netmon in the advanced methods section.

If you have multiple offices, you'll need to keep a set of data from a client in each of those locations as well. This test measures latency, which, in this case, is a number value that describes the amount of time between a client sending a request to Office 365, and Office 365 responding to the request. The testing originates inside your domain on a client computer, and looks to measure a round trip from inside your network, out through an egress point, across the Internet to Office 365, and back.

There are a few ways to deal with the egress point, in this case, the proxy server. You can either trace from 1 to 2 and then 2 to 3, and then add the numbers in milliseconds to get a final total to the edge of your network. Or, you can configure the connection to bypass the proxy for Office 365 addresses. In a larger network with a firewall, reverse proxy, or some combination of the two, you may need to make exceptions on the proxy server that will allow traffic to pass for a lot of URLs. For the list of endpoints used by Office 365, see [Office 365 URLs and IP address ranges](#). If you have an authenticating proxy, begin by testing exceptions for the following:

- Ports 80 and 443
- TCP and HTTPs

- Connections that are outbound to any of these URLs:
- *.microsoftonline.com
- *.microsoftonline-p.com
- *.sharepoint.com
- *.outlook.com
- *.lync.com
- osub.microsoft.com

All users need to be allowed to get to these addresses without any proxy interference or authentication. On a smaller network, you should add these to your proxy bypass list in your web browser.

To add these to your proxy bypass list in Internet Explorer, go to **Tools > Internet Options > Connections > LAN settings > Advanced**. The advanced tab is also where you will find your proxy server and proxy server port. You may need to click the checkbox **Use a proxy server for your LAN**, to access the **Advanced** button. You'll want to make sure that **Bypass proxy server for local addresses** is checked. Once you click **Advanced**, you'll see a text box where you can enter exceptions. Separate the wildcard URLs listed above with semi-colons, for example:

*.microsoftonline.com; *.sharepoint.com

Once you bypass your proxy, you should be able to use ping or PsPing directly on an Office 365 URL. The next step will be to test ping **outlook.office365.com**. Or, if you're using PsPing or another tool that will let you supply a port number to the command, PsPing against **portal.microsoftonline.com:443** to see the average round-trip time in milliseconds.

The round-trip time, or RTT, is a number value that measures how long it takes to send an HTTP request to a server like outlook.office365.com and get a response back that acknowledges the server knows that you did it. You'll sometimes see this abbreviated as RTT. This should be a relatively short amount of time.

You have to use **PsPing** or another tool that does not use ICMP packets that are blocked by Office 365 in order to do this test.

How to use PsPing to get an overall round trip time in milliseconds directly from an Office 365 URL

1. Run an elevated command prompt by completing these steps:
2. Click **Start**.
3. In the **Start Search** box, type cmd, and then press CTRL+SHIFT+ENTER.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. Navigate to the folder where the tool (in this case PsPing) is installed and test these Office 365 URLs:
 - psping admin.microsoft.com:443
 - psping microsoft-my.sharepoint.com:443
 - psping outlook.office365.com:443
 - psping www.yammer.com:443

```

C:\Perf>psping microsoft-my.sharepoint.com:443

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

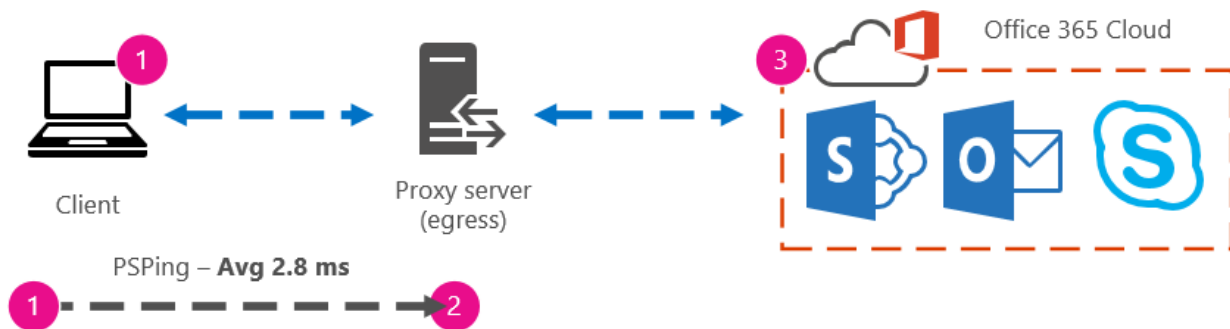
TCP connect to 2a01:111:f402:340d::14:443:
5 iterations (warmup 1) connecting test:
Connecting to 2a01:111:f402:340d::14:443 (warmup): 51.42ms
Connecting to 2a01:111:f402:340d::14:443: 53.63ms
Connecting to 2a01:111:f402:340d::14:443: 51.41ms
Connecting to 2a01:111:f402:340d::14:443: 50.84ms
Connecting to 2a01:111:f402:340d::14:443: 51.48ms

TCP connect statistics for 2a01:111:f402:340d::14:443:
Sent = 4, Received = 4, Lost = 0 (0% loss),
Minimum = 50.84ms, Maximum = 53.63ms, Average = 51.84ms

C:\Perf>

```

Be sure to include the port number of 443. Remember that Office 365 works on an encrypted channel. If you PsPing without the port number, your request will fail. Once you've pinged your short list, look for the Average time in milliseconds (ms). That is what you want to record!



If you're not familiar with proxy bypass, and prefer to take things step by step, you need to first find out the name of your proxy server. In Internet Explorer, go to **Tools > Internet Options > Connections > LAN settings > Advanced**. The **Advanced** tab is where you will see your proxy server listed. Ping that proxy server at a command prompt by completing this task:

To ping the proxy server and get a round trip value in milliseconds for stage 1 to 2

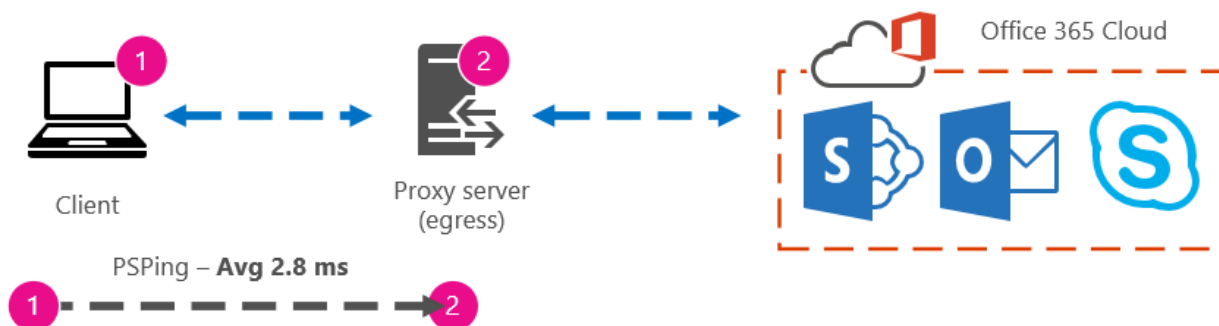
1. Run an elevated command prompt by completing these steps:
2. Click **Start**.
3. In the **Start Search** box, type cmd, and then press CTRL+SHIFT+ENTER.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. Type ping <the name of the proxy server your browser uses, or the IP address of the proxy server> and then press ENTER. If you have PsPing, or some other tool, installed, you can choose to use that tool instead.

Your command may look like any of these examples:

- ping ourproxy.ourdomain.industry.business.com
- ping 155.55.121.55
- ping ourproxy
- psping ourproxy.ourdomain.industry.business.com:80
- psping 155.55.121.55:80
- psping ourproxy:80

- When the trace stops sending test packets, you'll get a small summary that lists an average, in milliseconds, and that's the value you are after. Take a screenshot of the prompt and save it using your naming convention. At this point it may also help to fill in the diagram with the value.

Maybe you've taken a trace in the early morning, and your client can get to the proxy (or whatever egress server exits to the Internet) quickly. In this case, your numbers may look like this:



If your client computer is one of the select few with access to the proxy (or egress) server, you can run the next leg of the test by remotely connecting to that computer, running the command prompt to PsPing to an Office 365 URL from there. If you don't have access to that computer, you can contact your network resources for help with the next leg and get exact numbers that way. If that's not possible, take a PsPing against the Office 365 URL in question and compare it to the PsPing or Ping time against your proxy server.

For example, if you have 51.84 milliseconds from the client to the Office 365 URL, and you have 2.8 milliseconds from the client to the proxy (or egress point), then you have 49.04 milliseconds from the egress to Office 365. Likewise, if you have a PsPing of 12.25 milliseconds from the client to the proxy during the height of the day, and 62.01 milliseconds from the client to the Office 365 URL, then your average value for the proxy egress to the Office 365 URL is 49.76 milliseconds.



In terms of troubleshooting, you may find something interesting just from keeping these baselines. For example, if you find that you generally have about 40 milliseconds to 59 milliseconds of latency from the proxy or egress point to the Office 365 URL, and have a client to proxy or egress point latency of about 3 milliseconds to 7 milliseconds (depending on the amount network traffic you're seeing during that time of day) then you will surely know something is problematic if your last three client to proxy or egress baselines show a latency of 45 milliseconds.

Advanced methods

If you really want to know what is happening with your Internet requests to Office 365, you need to become familiar with network traces. It does not matter which tools you prefer for these traces, HTTPWatch, Netmon, Message Analyzer, Wireshark, Fiddler, Developer Dashboard tool or any other will do as long as that tool can capture and filter network traffic. You'll see in this section that it's beneficial to run more than one of these tools to get a more complete picture of the problem. When you're testing, some of these tools also act as proxies in their own right. Tools used in the companion article, [Performance troubleshooting plan for Office 365](#), include [Netmon 3.4](#), [HTTPWatch](#), or [WireShark](#).

Taking a performance baseline is the simple part of this method, and many of the steps are the same as when you troubleshoot a performance issue. The more advanced methods of creating baselines for performance require you to take and store network traces. Most of the examples in this article use SharePoint Online, but you should develop a list of common actions across the Office 365 services to which you subscribe to test and

record. Here is a baseline example:

- Baseline list for SPO - **** Step 1: **** Browse the home page of the SPO website and do a network trace. Save the trace.
- Baseline list for SPO - **Step 2:** Search for a term (such as your company name) via Enterprise Search and do a network trace. Save the trace.
- Baseline list for SPO - **Step 3:** Upload a large file to a SharePoint Online document library and do a network trace. Save the trace.
- Baseline list for SPO - **Step 4:** Browse the home page of the OneDrive website and do a network trace. Save the trace.

This list should include the most important common actions that users take against SharePoint Online. Notice that the last step, to trace going to OneDrive for Business, builds-in a comparison between the load of the SharePoint Online home page (which is often customized by companies) and OneDrive for Business home page, which is seldom customized. This is a basic test when it comes to a slow-loading SharePoint Online site. You can build a record of this difference into your testing.

If you are in the middle of a performance problem, many of the steps are the same as when taking a baseline. Network traces become critical, so we'll handle *how* to take the important traces next.

To tackle a performance problem, *right now*, you need to be taking a trace at the time you are experiencing the performance issue. You need to have the proper tools available to gather logs, and you need an action plan, that is, a list of troubleshooting actions to take to gather the best information that you can. The first thing to do is record the date and time of the test so that the files can be saved in a folder that reflect the timing. Next, narrow down to the problem steps themselves. These are the exact steps you will use for testing. Don't forget the basics: if the issue is only with Outlook, make sure to record that the problem behavior happens in only one Office 365 service. Narrowing down the scope of this issue will help you to focus on something you can resolve.

See also

[Managing Office 365 endpoints](#)

Tune Exchange Online performance

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article contains general tips and links to other resources that tell you how to improve performance of Exchange Online, particularly in front of a migration. This article is part of the [Network planning and performance tuning for Office 365](#) project.

Things to consider in order to improve Exchange Online performance

To improve the speed of migration and reduce your organization's bandwidth constraints for Exchange Online, consider the following:

- **Reduce mailbox sizes.** Smaller mailbox size improves migration speed.
- **Use the mailbox move capabilities with an Exchange hybrid deployment.** With an Exchange hybrid deployment, offline mail (in the form of .OST files) does not require re-download when migrating to Exchange Online. This significantly reduces your download bandwidth requirements.
- **Schedule mailbox moves to occur during periods of low Internet traffic and low on-premises Exchange use.** When scheduling moves, migration requests are submitted to the mailbox replication proxy and may not take place immediately.
- **Use lean popouts for Outlook on the web.** Lean popouts provide smaller, less memory-intensive versions of certain email messages in Microsoft Edge or Internet Explorer by rendering some components on the server. For more information, see [Use lean popouts to reduce memory used when reading mail messages](#).

General advice

- Make certain that DNS lookup for outlook.office.com enters the MS-datacenter at a logical entry location for your location.
- Research mailbox caching and choose the appropriate options (re. caching period, shared mailbox caching, et cetera).
- Keep your Outlook data from passing over VPN connections (to a central office) before it goes over the Internet.
- Be sure your mailbox data adheres to the limitations on folder, and item, amounts.

For more information about Exchange migration performance, see [Office 365 migration performance and best practices](#).

Tune SharePoint Online performance

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article contains links to other articles that tell you how to improve performance of page download times for SharePoint Online. This article is part of the [Network planning and performance tuning for Office 365](#) project.

Articles about fine tuning SharePoint Online performance

Use these articles to fine tune SharePoint Online performance.

- [Introduction to performance tuning for SharePoint Online](#)
- [Use the Page Diagnostics tool for SharePoint Online](#)
- [Navigation options for SharePoint Online](#)
- [Performance guidance for SharePoint Online portals](#)
- [Image optimization for SharePoint Online](#)
- [Delay loading images and JavaScript in SharePoint Online](#)
- [Minification and bundling in SharePoint Online](#)
- [Use the Office 365 Content Delivery Network \(CDN\) with SharePoint Online](#)
- [Using Content Search Web Part instead of Content Query Web Part to improve performance in SharePoint Online](#)
- [Capacity planning and load testing SharePoint Online](#)
- [Diagnosing performance issues with SharePoint Online](#)
- [Using the object cache with SharePoint Online](#)
- [How to: Avoid getting throttled or blocked in SharePoint Online](#)
- [Optimize iFrames in SharePoint Online modern portal pages](#)
- [Optimize web part performance in SharePoint Online modern portal pages](#)
- [Optimize page calls in SharePoint Online modern portal pages](#)
- [Optimize page weight in SharePoint Online modern portal pages](#)
- [Optimize images in SharePoint Online modern portal pages](#)

Introduction to performance tuning for SharePoint Online

10/28/2022 • 4 minutes to read • [Edit Online](#)

This article explains what specific aspects you need to consider when designing pages for best performance in SharePoint Online.

SharePoint Online metrics

The following broad metrics for SharePoint Online provide real-world data about performance:

- How fast pages load
- How many round-trips required per page
- Issues with the service
- Other things that cause performance degradation

Conclusions reached because of the data

The data tells us:

- Most of the pages perform well on SharePoint Online.
- Non-customized pages load quickly.
- OneDrive for Business, team sites and system pages, such as _layouts, etc., are all quick to load.
- The slowest 1% of SharePoint Online pages take more than 5,000 milliseconds to load.

One simple benchmark test you can use would be to measure performance by comparing the load time of your own portal against the load time of the OneDrive for Business home page as it uses few customized features. This will often be the first step Support will ask you to complete when troubleshooting network performance issues.

Use a standard user account when checking performance

A Site Collection Administrator, Site Owner, Editor, or Contributor belong to another security groups, have more permissions, and therefore have extra elements that SharePoint loads on a page.

This is applicable to SharePoint on-premises and SharePoint Online but in an on-premises scenario the differences will not be as easily noticed as in SharePoint Online.

In order to correctly evaluate how a page will perform for users, you should use a standard user account to avoid loading the authoring controls and extra traffic related to security groups.

Connection categories for performance tuning

You can categorize the connections between the server and the user into three main components. Consider these when designing SharePoint Online pages for insight into load times.

- **Server** The servers that Microsoft hosts in datacenters.
- **Network** The Microsoft network, the Internet, and your on-premises network between the datacenter

and your users.

- **Browser** Where the page is loaded.

Within these three connections there are typically five reasons that cause 95% of slow pages. Each of these reasons is discussed in this article:

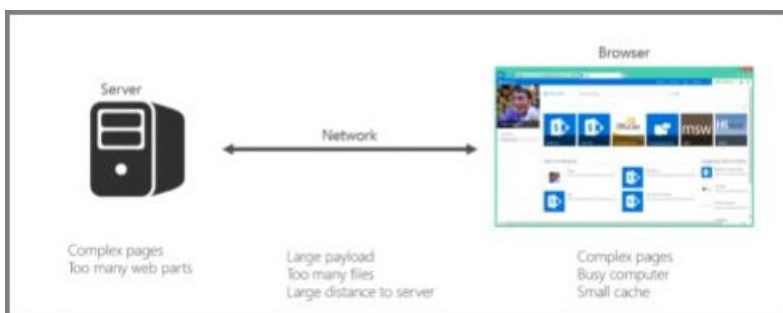
- Navigation issues
- Content roll-up
- Large files
- Many requests to the server
- Web Part processing

Server connection

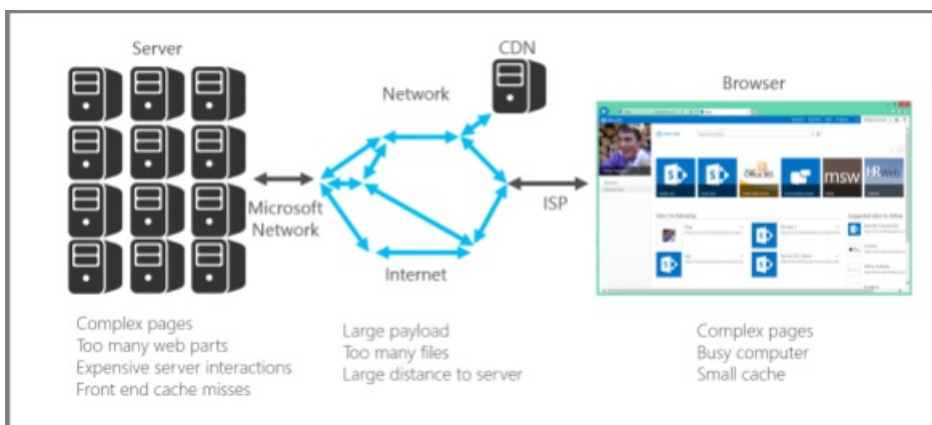
Many of the issues that affect performance with SharePoint on-premises also apply to SharePoint Online.

As you would expect, you have far more control over how servers perform with on-premises SharePoint. With SharePoint Online things are a little different. The more work you make a server do, the longer it takes to render a page. With SharePoint, the biggest culprits in this respect are complex pages with multiple web parts.

SharePoint Server on-premises



SharePoint Online



With SharePoint Online, certain page requests may actually end up calling multiple servers. You could end up with a matrix of requests between servers for an individual request. These interactions are expensive from a page load perspective and will make things slow.

Examples of these server-to-server interactions are:

- Web to SQL Servers
- Web to application servers

The other thing that can slow down server interactions is cache misses. Unlike on-premises SharePoint, there is

a slim chance that you will hit the same server for a page that you have visited previously; this makes object caching obsolete.

Network connection

With on-premises SharePoint that doesn't make use of a WAN, you may use a high-speed connection between datacenter and end users. Generally, things are easy to manage from a network perspective.

With SharePoint Online, there are a few more factors to consider; for example:

- The Microsoft network
- The Internet
- The ISP

Regardless of which version of SharePoint (and which network) you are using, things that will typically cause the network to be busy include:

- Large payload
- Many files
- Large physical distance to the server

One feature that you can use in SharePoint Online is the Microsoft CDN (Content Delivery Network). A CDN is basically a distributed collection of servers deployed across multiple datacenters. With a CDN, content on pages can be hosted on a server close to the client even if the client is far away from the originating SharePoint Server. Microsoft will be using this more in the future to store local instances of pages that cannot be customized, for example the SharePoint Online admin home page. For more information about CDNs, see [Content delivery networks](#).

Something that you need to be aware of but may not be able to do much about is the connection speed of your ISP. A simple speed test tool will tell you the connection speed.

Browser connection

There are a few factors to consider with web browsers from a performance perspective.

Visiting complex pages will affect performance. Most browsers only have a small cache (around 90 MB), while the average web page is typically around 1.6 MB. This doesn't take long to get used up.

Bandwidth may also be an issue. For example, if a user is watching videos in another session, this will affect the performance of your SharePoint page. While you can't prevent users from streaming media, you can control the way a page will load for users.

Check out the following articles for different SharePoint Online page customization techniques and other best practices to help you achieve optimal performance.

- [Navigation options for SharePoint Online](#)
- [Use the Page Diagnostics tool for SharePoint Online](#)
- [Image optimization for SharePoint Online](#)
- [Delay loading images and JavaScript in SharePoint Online](#)
- [Minification and bundling in SharePoint Online](#)
- [Use the Office 365 Content Delivery Network \(CDN\) with SharePoint Online](#)
- [Using Content Search Web Part instead of Content Query Web Part to improve performance in SharePoint Online](#)

- [Capacity planning and load testing SharePoint Online](#)
- [Diagnosing performance issues with SharePoint Online](#)
- [Using the object cache with SharePoint Online](#)
- [How to: Avoid getting throttled or blocked in SharePoint Online](#)

Diagnosing performance issues with SharePoint Online

10/28/2022 • 4 minutes to read • [Edit Online](#)

This article shows you how you can diagnose common issues with your SharePoint Online site using Internet Explorer developer tools.

There are four different ways that you can identify that a page on a SharePoint Online site has a performance problem with the customizations.

- The Site and Page performance diagnostic
- The F12 tool bar network monitor
- Comparison to a non-customized baseline
- SharePoint Online response header metrics

This topic describes how to use each of these methods to diagnose performance issues. Once you've figured out the cause of the problem, you can work toward a solution using the articles about improving SharePoint performance that you can find on <https://aka.ms/tune>.

Use the Site and Page performance diagnostic from the Microsoft 365 Admin Center

NOTE

If you're an administrator, and you're having trouble with performance in SharePoint, select **Run Tests** below, which will populate the Site and Page Performance diagnostic in the Microsoft 365 Admin Center. These tests will check your configuration and quickly recommend next steps to help improve SharePoint performance for your tenant.

[Run Tests: Check SharePoint Performance](#)

NOTE

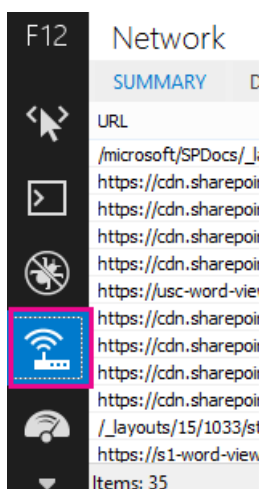
This feature is not available for Microsoft 365 Government, Microsoft 365 operated by 21Vianet, or Microsoft 365 Germany.

Using the F12 tool bar to diagnose performance in SharePoint Online

In this article, we use Internet Explorer 11. Versions of the F12 developer tools on other browsers have similar features though they may look slightly different. For information on the F12 developer tools, see:

- [What's new in F12 Tools](#)
- [Using the F12 developer tools](#)

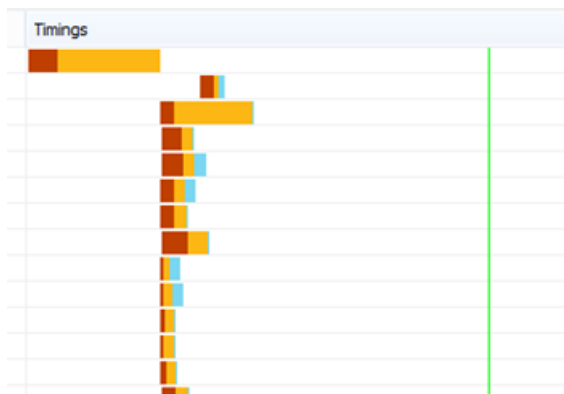
To bring up the developer tools press **F12** and then click the Wi-Fi icon:



On the **Network** tab, press the green play button to load a page. The tool returns all of the files that the browser requests in order to get the page you asked for. The following screenshot shows one such list.

URL
https://www.outlook.com/owa/?exch=1
https://sperformance.sharepoint.com/sites/NavigationBySearch/SitePages/Home.aspx
https://sperformance.sharepoint.com/sites/NavigationBySearch/SitePages/Home.aspx
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/js/jquery.easing.1.3.js
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/js/jquery.1.5.1.min.js
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/js/aad.login.js
https://secure.aadcdn.microsoftonline-p.com/aad/20.200.19625/css/login.ltr.css
https://prod.msocdn.com/16.00.0458.005/en-US/JSC/O365ShellPlus.js
https://prod.msocdn.com/16.00.0458.005/en-US/JSC/CoreShellBundle.js
https://prod.msocdn.com/16.00.0458.005/en-US/JSC/CoreShellBundle.js
https://prod.msocdn.com/16.00.0458.005/en-US/css/shellg1pluscss_7ae920ff.css
https://prod.msocdn.com/16.00.0458.005/en-US/css/shellg1corecss_55f6794d.css
https://prod.msocdn.com/16.00.0458.005/en-US/css/shelleoticons_f48736e7.eot?#iefix
https://portal.office.com/SuiteServiceProxy.aspx?exsvurl=1&realm=office365.com&Silent=1
https://portal.office.com/SuiteServiceProxy.aspx?exsvurl=1&realm=office365.com

You can also see the download times of the files on the right side as shown in this screenshot.



This gives you a visual representation of how long the file took to load. The green line represents when the page is ready to be rendered by the browser. This can give you a quick view of the different files that might be causing slow page loads on your site.

Setting up a non-customized baseline for SharePoint Online

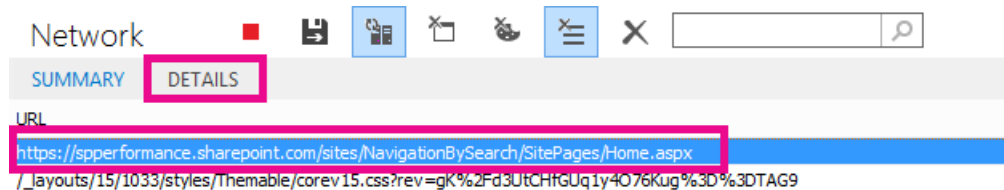
The best way to determine your site's performance weak points is to set up a completely out-of-the-box site collection in SharePoint Online. This way you can compare all the various aspects of your site with what you would get with no customization on the page. The OneDrive for Business home page is a good example of a separate site collection that is unlikely to have any customizations.

Viewing SharePoint response header information

In SharePoint Online, you can access the information that is sent back to the browser in the response header for each file. The most useful value for diagnosing performance issues is **SPRequestDuration**, which displays the amount of time that the request took on the server to be processed. This can help determine if the request is heavy and resource intensive. This is the best insight you have into how much work the server is doing to serve the page.

To view SharePoint response header information

1. Ensure that you have the F12 tools installed. For more information on downloading and installing these tools, see [What's new in F12 tools](#).
2. In the F12 tools, on the **Network** tab, press the green play button to load a page.
3. Click one of the .aspx files returned by the tool and then click **DETAILS**.



4. Click **Response headers**.

Request headers	Request body	Response headers	Response body
Key		Value	
Response		HTTP/1.1 200 OK	
Cache-Control		private, max-age=86400	
Content-Type		text/html; charset=utf-8	
Expires		Tue, 21 Oct 2014 21:47:52 GMT	
Server		Microsoft-IIS/7.5	
Set-Cookie		rtFa=EOjag36aM1ndJa+hufHEv	
Set-Cookie		FedAuth=77u/PD94bWwgdMvy	
X-AspNet-Version		4.0.30319	
SPRequestGuid		4b1bc49c-6003-1000-8be7-ff15	
request-id		4b1bc49c-6003-1000-8be7-ff15	
X-FRAME-OPTIONS		SAMEORIGIN	
SPRequestDuration		71	
SPIIsLatency		0	
X-Powered-By		ASP.NET	
MicrosoftSharePointTeamServices		16.0.0.3312	
X-Content-Type-Options		nosniff	
X-MS-InvokeApp		1; RequireReadOnly	
P3P		CP="ALL IND DSP COR ADM CO	
Date		Mon, 20 Oct 2014 21:47:51 GMT	
Content-Length		21059	

What's causing performance issues in SharePoint Online?

The article [Navigation options for SharePoint Online](#) shows an example of using the **SPRequestDuration** value to determine that the complicated structural navigation was causing the page to take a long time to process on the server. By taking a value for a baseline site (without customization), it's possible to determine if any given file is taking a long time to load. The example used in [Navigation options for SharePoint Online](#) is the main .aspx file. That file contains most of the ASPNET code that runs for your page load. Depending on the site template you use, this could be start.aspx, home.aspx, default.aspx, or another name if you customize the home page. If this number is considerably higher than your baseline site, then it's a good indication that there's something complex going on in your page that is causing performance issues.

Once you've identified that an issue specific to your site, the recommended way to figure out what is causing poor performance is to eliminate all of the possible causes, like page customizations, and then add them back to the site one by one. Once you have removed enough customizations that the page is performing well, you can then add back specific customizations one by one.

For example, if you have a complex navigation try changing the navigation to not show sub-sites then check the developer tools to see if this makes a difference. Or if you have a large amount of content roll-ups try removing them from your page and see if this improves things. If you eliminate all of the possible causes and add them back in one at a time, you can easily identify which features are the biggest problem and then work towards a solution.

Performance troubleshooting plan for Office 365

10/28/2022 • 31 minutes to read • [Edit Online](#)

Do you need to know the steps to take to identify and fix lags, hangs, and slow performance between SharePoint Online, OneDrive for Business, Exchange Online, or Skype for Business Online, and your client computer? Before you call support, this article can help you troubleshoot Office 365 performance issues and even fix some of the most common issues.

This article is actually a sample action plan that you can use to capture valuable data about your performance issue as it's happening. Some top issues are also included in this article.

If you're new to network performance and want to make a long term plan to monitor performance between your client machines and Office 365, take a look at [Office 365 performance tuning and troubleshooting - Admin and IT Pro](#).

Sample performance troubleshooting action plan

This action plan contains two parts; a preparation phase, and a logging phase. If you have a performance problem right now, and you need to do data collection, you can start using this plan right away.

Prepare the client computer

- Find a client computer that can reproduce the performance problem. This computer will be used during troubleshooting.
- Write down the steps that cause the performance problem to happen so you're ready when it comes time to test.
- Install tools for gathering and recording information:
 - Install [Netmon 3.4](#) (or use an equivalent network tracing tool).
 - Install the free Basic Edition of [HTTPWatch](#) (or use an equivalent network Tracing tool).
 - Use a screen recorder or run the Steps Recorder (PSR.exe) that comes with Windows Vista and later, in order to keep a record of the steps you take during testing.

Log the performance issue

- Close all extraneous Internet browsers.
- Start the Steps Recorder, or another screen recorder.
- Start your Netmon capture (or network tracing tool).
- Clear your DNS cache on the client computer from the command line by typing `ipconfig /flushdns`.
- Start a new browser session and turn on HTTPWatch.
- Optional: If you're testing Exchange Online, run the Exchange Client Performance Analyzer tool from the Office 365 admin console.
- Reproduce the exact steps that cause the performance issue.
- Stop your Netmon or other tool's trace.
- At the command line, run a trace route to your Office 365 subscription by typing the following command and then pressing ENTER:


```
tracert <subscriptionname>.onmicrosoft.com
```

- Stop the Steps Recorder and save the video. Be sure to include the date and time of the capture and whether it demonstrates good or bad performance.
- Save the trace files. Again, be sure to include the date and time of the capture and whether it demonstrates good or bad performance.

If you're not familiar with running the tools mentioned in this article, don't worry because we provide those steps next. If you're accustomed to doing this kind of network capturing, you can skip to [How to collect baselines](#), which describes filtering and reading the logs.

Flush the DNS Cache first

Why? By flushing out the DNS cache, you're starting your tests with a clean slate. By clearing the cache, you're resetting the DNS resolver contents to the most up-to-date entries. Remember that a flush doesn't remove HOST file entries. If you use HOST file entries extensively, you should copy those entries out to a file in another directory and then empty the HOST file.

Flush your DNS resolver cache

1. Open the command prompt, (either **Start > Run > cmd** or **Windows key > cmd**).
2. Type the following command and press ENTER:

```
ipconfig /flushdns
```

Netmon

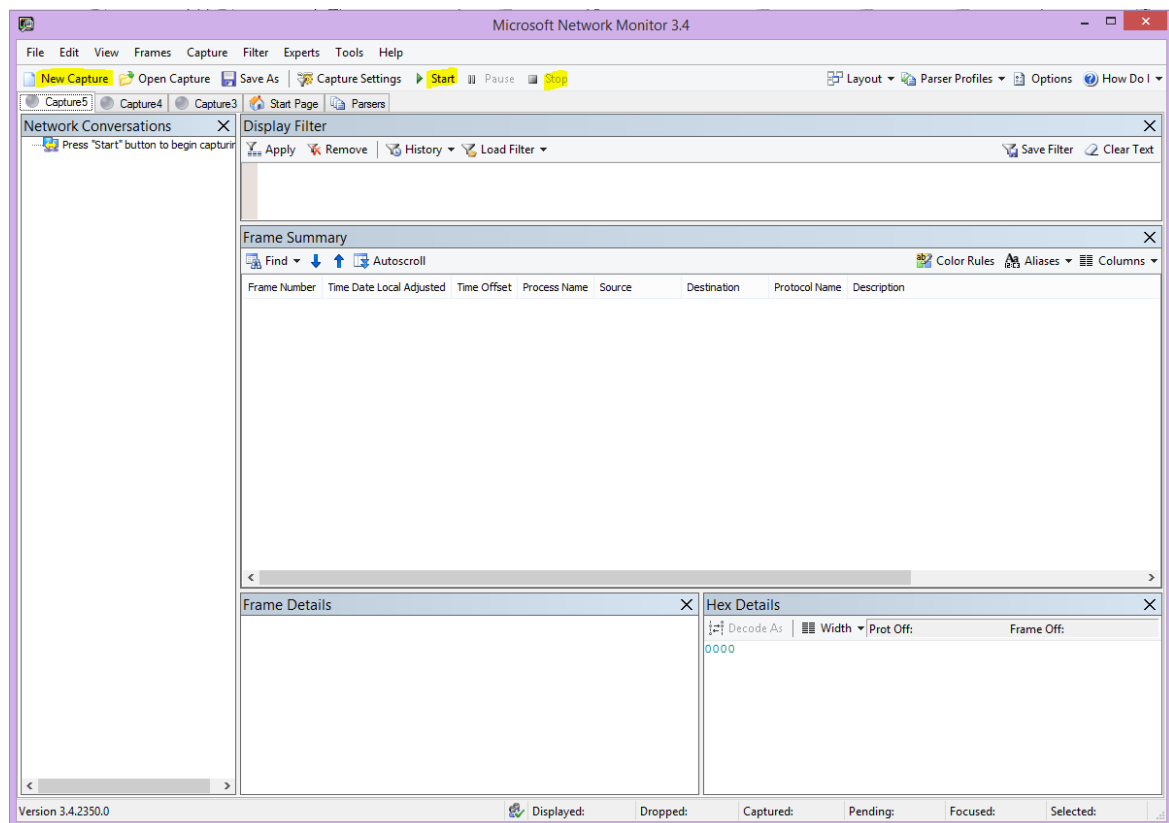
Microsoft's Network Monitoring tool ([Netmon](#)) analyzes packets, that is traffic, that passes between computers on networks. By using Netmon to trace traffic with Office 365 you can capture, view, and read packet headers, identify intervening devices, check important settings on network hardware, look for dropped packets, and follow the flow of traffic between computers on your corporate network and Office 365. Because the actual body of the traffic is encrypted, that is, it travels on port 443 via SSL/TLS, you can't read the files being sent. Instead, you get an unfiltered trace of the path that the packet takes which can help you track down the problem behavior.

Be sure you don't apply a filter at this time. Instead, run through the steps and demonstrate the problem before stopping the trace and saving.

After you install Netmon 3.4, open the tool and take these steps:

Take a Netmon trace and reproduce the issue

1. Launch Netmon 3.4. There are three panes on the **Start** page: **Recent Captures**, **Select Networks**, and the **Getting Started with Microsoft Network Monitor 3.4. Notice**. The Select Networks panel will also give you a list of the default networks from which you can capture. Be sure that network cards are selected here.
2. Click **New Capture** at the top of the **Start** page. This adds a new tab beside the **Start** page tab called **Capture 1**.



3. To take a simple capture, click **Start** on the toolbar.
4. Reproduce the steps that present a performance issue.
5. Click **Stop** > **File** > **Save As**. Remember to give the date and time with the time zone and to mention if it demonstrates bad or good performance.

HTTPWatch

[HTTPWatch](#) comes in charged, and a free edition. The free Basic Edition covers everything you need for this test. HTTPWatch monitors network traffic and page load time right from your browser window. HTTPWatch is a plug-in to Internet Explorer that graphically describes performance. The analysis can be saved and viewed in HTTPWatch Studio.

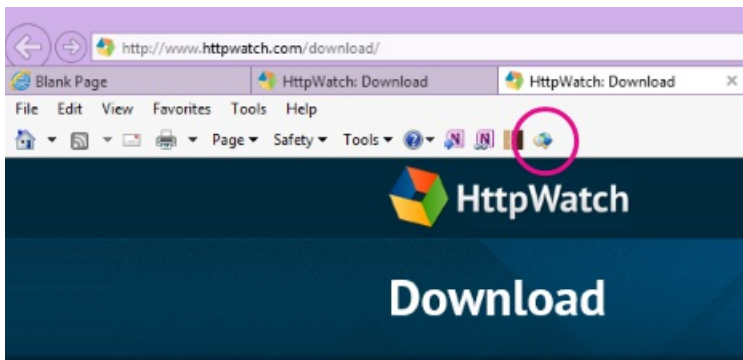
NOTE

If you use another browser, such as Firefox, Google Chrome, or if you can't install HTTPWatch in Internet Explorer, open a new browser window and press F12 on your keyboard. You should see the Developer Tool pop-up at the bottom of your browser. If you use Opera, press CTRL+SHIFT+I for Web Inspector, then click the **Network** tab and complete the testing outlined below. The information will be slightly different, but load times will still be displayed in milliseconds. > HTTPWatch is also very useful for issues with SharePoint Online page load times.

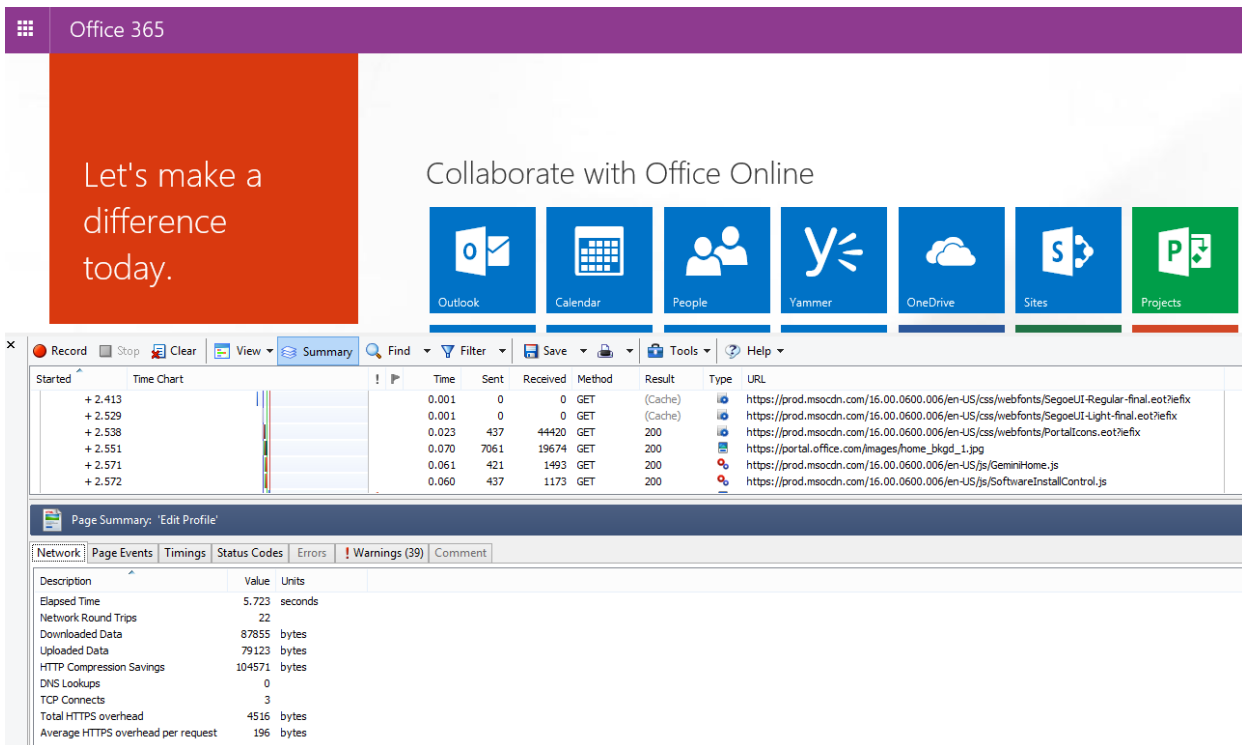
Run HTTPWatch and reproduce the issue

HTTPWatch is a browser plug-in, so exposing the tool in the browser is slightly different for each version of Internet Explorer. Typically, you can find HTTPWatch under the Commands bar in the Internet Explorer browser. If you don't see the HTTPWatch plug-in in your browser window, check the version of your browser by clicking **Help** > **About**, or in later versions of Internet Explorer, click the gear symbol and **About Internet Explorer**. To launch the **Commands** bar, right-click the menu bar in Internet Explorer and click **Commands bar**.

In the past, HTTPWatch has been associated with both the Commands and the Explorer bars, so once you install, if you don't immediately see the icon (even after reboot) check **Tools**, and your toolbars for the icon. Remember that toolbars can be customized and options can be added to them.



1. Launch HTTPWatch in an Internet Explorer browser window. It will appear docked to the browser at the bottom of that window. Click **Record**.
2. Reproduce the exact steps involved in the performance issue. Click the **Stop** button in HTTPWatch.
3. **Save** the HTTPWatch or **Send by Email**. Remember to name the file so that it includes date and time information and an indication of whether your Watch contains a demonstration of good or bad performance.



This screenshot is from the Professional version of HTTPWatch. You can open traces taken in the Basic Version on a computer with a Professional version and read it there. Extra information may be available from the trace through that method.

Problem Steps Recorder

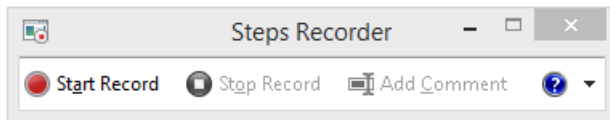
Steps Recorder, or PSR.exe, allows you to record issues as they're occurring. It's a very useful tool and simple to run.

Run Problem Steps Recorder (PSR.exe) to record your work

1. Either use **Start > Run > type PSR.exe > OK**, or, click the **Windows Key > type PSR.exe >** and then press **ENTER**.
2. When the small PSR.exe window appears, click **Start Record** and reproduce the steps that reproduce the performance issue. You can add comments as needed, by clicking **Add Comments**.
3. Click **Stop Record** when you've completed the steps. If the performance issue is a page render, wait for

the page to render before you stop the recording.

4. Click **Save**.



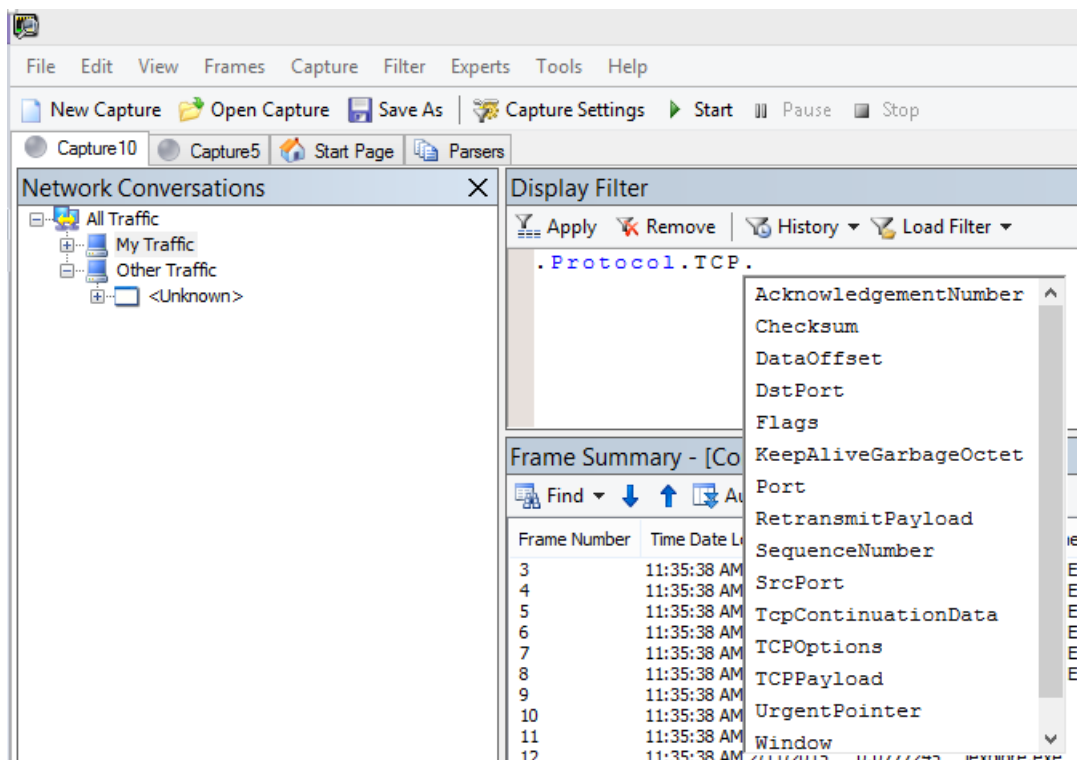
The date and time is recorded for you. This links your PSR to your Netmon trace and HTTPWatch in time, and helps with precision troubleshooting. The date and time in the PSR record can show that a minute passed between the login and browsing of the URL and the partial render of the admin site, for example.

Read your traces

It isn't possible to teach everything about network and performance troubleshooting that someone would need to know via an article. Getting good at performance takes experience, and knowledge of how your network works and usually performs. But it's possible to round up a list of top issues and show how tools can make it easier for you to eliminate the most common problems.

If you want to pick up skills reading network traces for your Office 365 sites, there's no better teacher than creating traces of page loads regularly and gaining experience reading them. For example, when you have a chance, load an Office 365 service and trace the process. Filter the trace for DNS traffic, or search the FrameData for the name of the service you browsed. Scan the trace to get an idea of the steps that occur when the service loads. This will help you learn what normal page load should look like, and in the case of troubleshooting, particularly around performance, comparing good to bad traces can teach you a lot.

Netmon uses Microsoft Intellisense in the Display filter field. Intellisense, or intelligent code completion, is that trick where you type in a period and all available options are displayed in a drop-down selection box. For example, you're worried about TCP window scaling, you can find your way to a filter (such as `.protocol.tcp.window < 100`) by this means.



Netmon traces can have a lot of traffic in them. If you aren't experienced with reading them, it's likely you'll be overwhelmed opening the trace the first time. The first thing to do is separate the signal from the background noise in the trace. You tested against Office 365, and that's the traffic you want to see. If you're used to

navigating through traces, you may not need this list.

Traffic between your client and Office 365 travels via TLS, which means that the body of the traffic will be encrypted and not readable in a generic Netmon trace. Your performance analysis doesn't need to know the specifics of the information in the packet. It is, however, very interested in packet headers and the information that they contain.

Tips to get a good trace

- Know the value of the IPv4 or IPv6 address of your client computer. You can get this from the command prompt by typing **IPConfig** and then pressing ENTER. Knowing this address will let you tell at a glance whether the traffic in the trace directly involves your client computer. If there's a known proxy, ping it and get its IP address as well.
- Flush your DNS resolver cache and, if possible, close all browsers except the one in which you're running your tests. If you aren't able to do this, for instance, if support is using some browser-based tool to see your client computer's desktop, be prepared to filter your trace.
- In a busy trace, locate the Office 365 service that you're using. If you've never or seldom seen your traffic before, this is a helpful step in separating the performance issue from other network noise. There are a few ways to do this. Directly before your test, you can use *ping* or *PsPing* against the URL of the specific service (`ping outlook.office365.com` OR `psping -4 microsoft-my.sharepoint.com:443` , for example). You can also easily find that ping or PsPing in a Netmon trace (by its process name). That will give you a place to start looking.

If you're only using Netmon tracing at the time of the problem, that's okay too. To orient yourself, use a filter like `ContainsBin(FrameData, ASCII, "office")` OR `ContainsBin(FrameData, ASCII, "outlook")` . You can record your frame number from the trace file. You may also want to scroll the *Frame Summary* pane all the way to the right and look for the Conversation ID column. There's a number indicated there for the ID of this specific conversation that you can also record and look at in isolation later. Remember to remove this filter before applying any other filtering.

TIP

Netmon has a lot of helpful built-in filters. Try the **Load Filter** button at the top of the *Display* filter pane.

```
C:\WINDOWS\system32\Cmd.exe

C:\Perf>psping outlook.office365.com:443

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 2a01:111:f400:1428::2:443:
5 iterations (warmup 1) connecting test:
Connecting to 2a01:111:f400:1428::2:443 (warmup): 5.80ms
Connecting to 2a01:111:f400:1428::2:443: 5.98ms
Connecting to 2a01:111:f400:1428::2:443: 6.24ms
Connecting to 2a01:111:f400:1428::2:443: 6.20ms
Connecting to 2a01:111:f400:1428::2:443: 6.43ms

TCP connect statistics for 2a01:111:f400:1428::2:443:
Sent = 4, Received = 4, Lost = 0 (0% loss),
Minimum = 5.98ms, Maximum = 6.43ms, Average = 6.21ms

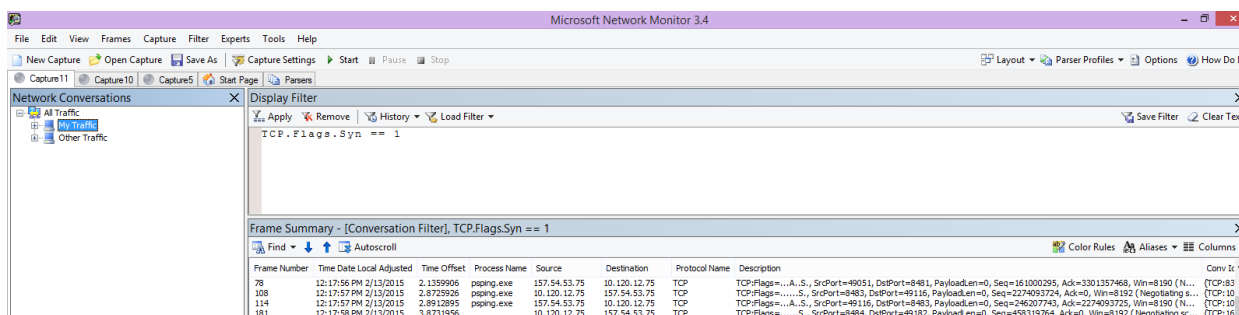
C:\Perf>psping -4 outlook.office365.com:443

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 132.245.92.34:443:
5 iterations (warmup 1) connecting test:
Connecting to 132.245.92.34:443 (warmup): 251.65ms
Connecting to 132.245.92.34:443: 9.12ms
Connecting to 132.245.92.34:443: 9.33ms
Connecting to 132.245.92.34:443: 9.15ms
Connecting to 132.245.92.34:443: 8.44ms

TCP connect statistics for 132.245.92.34:443:
Sent = 4, Received = 4, Lost = 0 (0% loss),
Minimum = 8.44ms, Maximum = 9.33ms, Average = 9.01ms

C:\Perf>
```



Get familiar with your traffic, and learn to locate the information you need. For example, learn to determine which packet in the trace has the first reference to the Office 365 service you're using (like "Outlook").

Taking Office 365 Outlook Online as an example, the traffic begins something like this:

- DNS Standard Query and DNS Response for outlook.office365.com with matching QueryIDs. It's important to note the time offset for this turn-around, and where in the world the Office 365 Global DNS sends the request for name resolution. Ideally, as locally as possible, rather than halfway across the world.
- An HTTP GET Request whose status report Moved Permanently (301)
- RWS Traffic including RWS Connect requests and Connect replies. (This is Remote Winsock making a connection for you.)
- A TCP SYN and TCP SYN/ACK conversation. Many settings in this conversation impact your performance.
- Then a series of TLS:TLS traffic, which is where the TLS handshake and TLS certificate conversations take place. (Remember the data is encrypted via SSL/TLS.)

All parts of the traffic are important and connected, but small portions of the trace contain information important in terms of performance troubleshooting, so we'll focus on those areas. Also, since we've done enough Office 365 performance troubleshooting at Microsoft to compile a Top Ten list of common problems, we'll focus on those issues and how to use the tools we have to root them out next.

If you haven't installed them already, the matrix below makes use of several tools where ever possible. Links are provided to the installation points. The list includes common network tracing tools like [Netmon](#) and [Wireshark](#), but use any tracing tool you're comfortable with, and in which you're accustomed to filtering network traffic. When you're testing, remember:

- *Close your browsers, and test with only one browser running* - This will reduce the overall traffic you capture. It makes for a less busy trace.
- *Flush your DNS resolver cache on the client computer* - This will give you a clean slate when you start to take your capture, for a cleaner trace.

Common issues

Some common issues you may face and how to find them in your Network trace.

TCP Windows Scaling

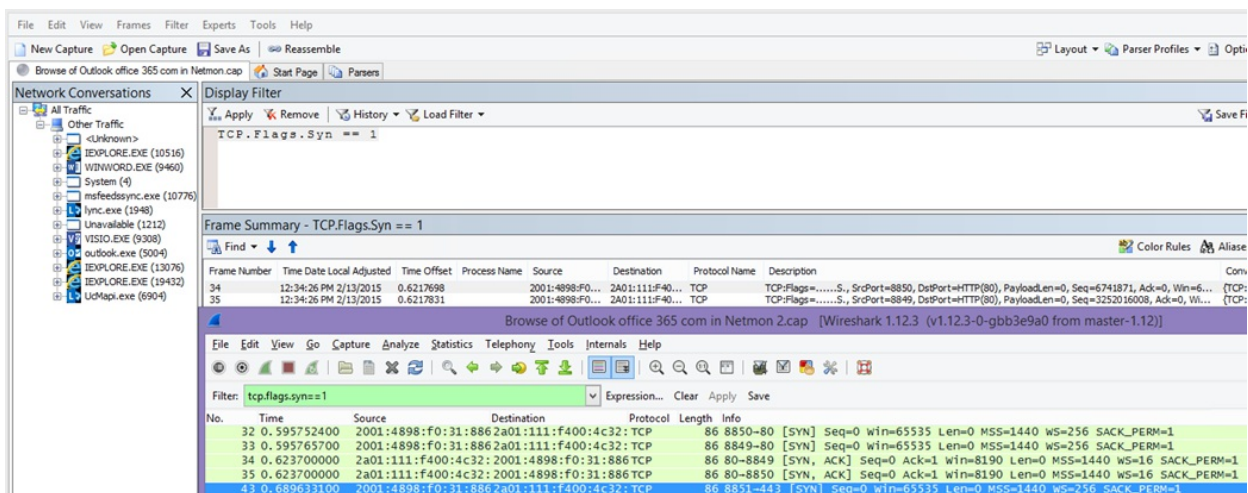
Found in the SYN - SYN/ACK. Legacy or aging hardware may not take advantage of TCP windows scaling. Without proper TCP windows scaling settings, the default 16-bit buffer in TCP headers fills in milliseconds. Traffic can't continue to send until the client receives an acknowledgment that the original data has been received, causing delays.

Tools

- Netmon
- Wireshark

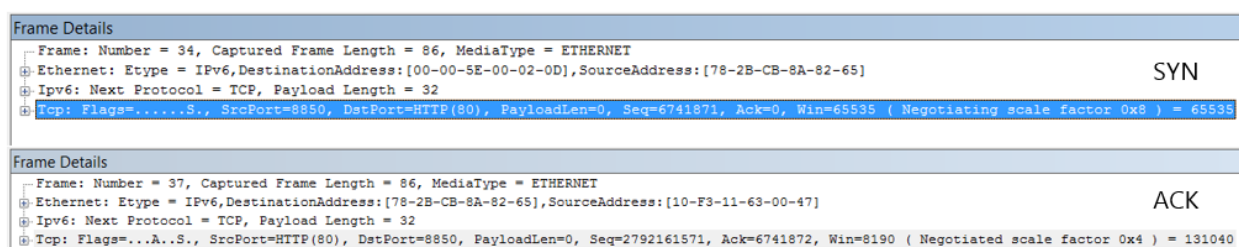
What to look for

Look for the SYN - SYN/ACK traffic in your network trace. In Netmon, use a filter like `tcp.flags.syn == 1`. This filter is the same in Wireshark.



Notice that for every SYN there's a source port (SrcPort) number that is matched in the destination port (DstPort) of the related Acknowledgment (SYN/ACK).

To see the Windows Scaling value that is used by your network connection, expand first the SYN, and then the related SYN/ACK.



TCP Idle Time Settings

Historically, most perimeter networks are configured for transient connections, meaning idle connections are generally terminated. Idle TCP sessions can be terminated by proxies and firewalls at greater than 100 to 300 seconds. This is problematic for Outlook Online because it creates and uses long-term connections, whether they're idle or not.

When connections are terminated by proxy or firewall devices, the client isn't informed, and an attempt to use Outlook Online will mean a client computer will try, repeatedly, to revive the connection before making a new one. You may see hangs in the product, prompts, or slow performance on page load.

Tools

- Netmon
- Wireshark

What to look for

In Netmon, look at the Time Offset field for a round-trip. A round-trip is the time between client sending a request to the server and receiving a response back. Check between the Client and the egress point (ex. Client --> Proxy), or the Client to Office 365 (Client --> Office 365). You can see this in many types of packets.

As an example, the filter in Netmon may look like

```
.Protocol.IPv4.Address == 10.102.14.112 AND .Protocol.IPv4.Address == 10.201.114.12 , or, in Wireshark,  
ip.addr == 10.102.14.112 && ip.addr == 10.201.114.12
```

TIP

Don't know if the IP address in your trace belongs to your DNS server? Try looking it up at the command line. Click **Start** > **Run** > and type **cmd**, or press **Windows Key** > and type **cmd**. At the prompt, type `nslookup <the IP address from the network trace>`. To test, use nslookup against your own computer's IP address. > To see a list of Microsoft's IP ranges, see [Office 365 URLs and IP address ranges](#).

If there's a problem, expect long Time Offsets to appear, in this case (Outlook Online), particularly in TLS:TLS packets that show the passage of Application Data (for example, in Netmon you can find application data packets via `.Protocol.TLS AND Description == "TLS:TLS Rec Layer-1 SSL Application Data"`). You should see a smooth progression in the time across the session. If you see long delays when refreshing your Outlook Online, this could be caused by a high degree of resets being sent.

Latency/Round Trip Time

Latency is a measure that can change a lot depending on many variables, such upgrading aging devices, adding a large number of users to a network, and the percentage of overall bandwidth consumed by other tasks on a network connection.

There are bandwidth calculators for Office 365 available from this [Network planning and performance tuning for Office 365](#) page.

Need to measure the speed of your connection, or your ISP connection's bandwidth? Try this site (or sites like it): [Speedtest Official Site](#), or query your favorite search engine for the phrase **speed test**.

Tools

- Ping
- PsPing
- Netmon
- Wireshark

What to look for

To track latency in a trace, you'll benefit from having recorded the client computer IP address and the IP address of the DNS server in Office 365. This is for easier trace filtering. If you connect through a proxy, you will need

your client computer IP address, the proxy/egress IP address, and the Office 365 DNS IP address, to make the work easier.

A ping request sent to outlook.office365.com will tell you the name of the datacenter receiving the request, even if ping *may* not be able to connect to send the trademark consecutive ICMP packets. If you use PsPing (a free tool for download), and specify the port (443) and perhaps to use IPv4 (-4) you will get an average round-trip-time for packets sent. This will work this for other URLs in the Office 365 services, like

`psping -4 yourSite.sharepoint.com:443`. In fact, you can specify a number of pings to get a larger sample for your average, try something like `psping -4 -n 20 yourSite-my.sharepoint.com:443`.

NOTE

PsPing doesn't send ICMP packets. It pings with TCP packets over a specific port, so you can use any one you know to be open. In Office 365, which uses SSL/TLS, try attaching port :443 to your PsPing.

```
C:\Perf>
C:\Perf>ping outlook.office365.com

Pinging outlook-namnorthwest.office365.com [2a01:111:f400:2c40::2] with 32 bytes
of data:
Request timed out.

Ping statistics for 2a01:111:f400:2c40::2:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Perf>psping -4 outlook.office365.com:443

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 132.245.92.194:443:
5 iterations (warmup 1) connecting test:
Connecting to 132.245.92.194:443 (warmup): 6.48ms
Connecting to 132.245.92.194:443: 6.66ms
Connecting to 132.245.92.194:443: 6.34ms
Connecting to 132.245.92.194:443: 6.47ms
Connecting to 132.245.92.194:443: 6.61ms

TCP connect statistics for 132.245.92.194:443:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Minimum = 6.34ms, Maximum = 6.66ms, Average = 6.52ms
C:\Perf>
```

If you loaded the slow performing Office 365 page while doing a network trace, you should filter a Netmon or Wireshark trace for `DNS`. This is one of the IPs we're looking for.

Here are the steps to take to filter your Netmon to get the IP address (and take a look at DNS Latency). This example uses outlook.office365.com, but may also use the URL of a SharePoint Online tenant (hithere.sharepoint.com for example).

1. Ping the URL `ping outlook.office365.com` and, in the results, record the name and IP address of the DNS server the ping request was sent to.
2. Network trace opening the page, or doing the action that gives you the performance problem, or, if you see a high latency on the ping, itself, network trace it.
3. Open the trace in Netmon and filter for DNS (this filter also works in Wireshark, but is sensitive to case `-- dns`). Since you know the name of the DNS server from your ping you may also filter more speedily in Netmon like this: `DNS AND ContainsBin(FrameData, ASCII, "namnorthwest")`, which looks like this in Wireshark dns and frame contains "namnorthwest".
Open the response packet and, in the Netmon **Frame Details** window, click **DNS** to expand for more information. In the DNS information you'll find the IP address of the DNS server the request went to in Office 365. You'll need this IP address for the next step (the PsPing tool). Remove the filter, right-click on the DNS Response in Netmon (**Frame Summary** > **Find Conversations** > **DNS**) to see the DNS Query and Response side-by-side.
4. In Netmon, also note the Time Offset column between the DNS Request and Response. In the next step, the easy-to-install and use [PsPing](#) tool comes in very handy, both because ICMP is often blocked on Firewalls,

and because PsPing elegantly tracks latency in milliseconds. PsPing completes a TCP connection to an address and port (in our case open port 443).

5. Install PsPing.
6. Open a command prompt (Start > Run > type cmd, or Windows Key > type cmd) and change directory to the directory where you installed PsPing to run the PsPing command. In my examples you can see I made a 'Perf' folder on the root of C. You can do the same for quick access.
7. Type the command so that you're making your PsPing against the IP address of the Office 365 DNS server from your earlier Netmon trace, including the port number, like `psping -n 20 132.245.24.82:443`. This will give you a sampling of 20 pings and average the latency when PsPing stops.

If you're going to Office 365 through a proxy server, the steps are a little different. You would first PsPing to your proxy server to get an average latency value in milliseconds to proxy/egress and back, and then either run PsPing on the proxy, or on a computer with a direct Internet connection to get the missing value (the one to Office 365 and back).

If you choose to run PsPing from the proxy, you'll have two millisecond values: Client computer to proxy server or egress point, and proxy server to Office 365. And you're done! Well, recording values, anyway.

If you run PsPing on another client computer that has a direct connection to the Internet, that is, without a proxy, you will have two millisecond values: Client computer to proxy server or egress point, and client computer to Office 365. In this case, subtract the value of client computer to proxy server or egress point from the value of client computer to Office 365, and you will have the RTT numbers from your client computer to the proxy server or egress point, and from proxy server or egress point to Office 365.

However, if you can find a client computer in the impacted location that is directly connected, or bypasses the proxy, you may choose to see if the issue reproduces there to begin with, and test using it thereafter.

Latency, as seen in a Netmon trace, those extra milliseconds can add up, if there are enough of them in any given session.

Frame Summary - [Conversation Filter]									
Find   									
Frame Number	Time Date Local Adjusted	Time Offset	Time Delta	Process Name	Source	Destination	Protocol Name	Description	
2	12:16:32 PM 3/4/2015	0.0000000	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=CE...S., SrcP	
3	12:16:32 PM 3/4/2015	0.2598509	0.2598509	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:Flags=...A...S., SrcP	
4	12:16:32 PM 3/4/2015	0.2606875	0.0008366	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=...A..., SrcPo	
5	12:16:32 PM 3/4/2015	0.2612543	0.0005668	IEXPLORE.EXE	10.164.114.89	10.190.224.84	HTTP	HTTP:Request, GET http:	
6	12:16:32 PM 3/4/2015	0.5527667	0.2915124	IEXPLORE.EXE	10.190.224.84	10.164.114.89	HTTP	HTTP:Response, HTTP/1.	
7	12:16:32 PM 3/4/2015	0.5527667	0.0000000	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:[Continuation to #6]f	
8	12:16:32 PM 3/4/2015	0.5528663	0.0000996	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=...A..., SrcPo	
9	12:16:32 PM 3/4/2015	0.8402279	0.2873616	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:[Continuation to #6]f	
10	12:16:32 PM 3/4/2015	0.8402279	0.0000000	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:[Continuation to #6]f	
11	12:16:32 PM 3/4/2015	0.8403318	0.0001039	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=...A..., SrcPo	
12	12:16:32 PM 3/4/2015	0.8406364	0.0003046	IEXPLORE.EXE	10.164.114.89	10.190.224.84	HTTP	HTTP:Request, GET http:	
13	12:16:32 PM 3/4/2015	0.8406364	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:[Continuation to #21	
14	12:16:32 PM 3/4/2015	0.8406364	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:[Continuation to #12	

NOTE

Your IP address may be different than the IPs shown here, for example, your ping may return something more like 157.56.0.0/16 or a similar range. For a list of ranges used by Office 365, check out [Office 365 URLs and IP address ranges](#).

Remember to expand all the nodes (there's a button at the top for this) if you want to search for, for example, 132.245.

Proxy Authentication

This only applies to you if you're going through a proxy server. If not, you can skip these steps. When working properly, proxy authentication should take place in milliseconds, consistently. You shouldn't see intermittent bad performance during peak usage periods (for example).

If Proxy authentication is on, each time you make a new TCP connection to Office 365 to get information, you

need to pass through an authentication process behind the scenes. So, for example, when switching from Calendar to Mail in Outlook Online, you will authenticate. And in SharePoint Online, if a page displays media or data from multiple sites or locations, you will authenticate for each different TCP connection that is needed in order to render the data.

In Outlook Online, you may experience slow load times whenever you switch between Calendar and your mailbox, or slow page loads in SharePoint Online. However, there are other symptoms not listed here.

Proxy authentication is a setting on your egress proxy server. If it is causing a performance issue with Office 365, you must consult your networking team.

Tools

- Netmon
- Wireshark

What to look for

Proxy authentication takes place whenever a new TCP session must be spun up, commonly to request files or info from the server, or to supply info. For example, you may see proxy authentication around HTTP GET or HTTP POST requests. If you want to see the frames where you are authenticating requests in your trace, add the 'NTLMSSP Summary' column to Netmon and filter for `.property.NTLMSSPSummary`. To see how long the authentication is taking, add the Time Delta column.

To add a column to Netmon:

1. Right-click on a column such as **Description**.
2. Click **Choose Columns**.
3. Locate *NTLMSSP Summary* and *Time Delta* in the list and click **Add**.
4. Move the new columns into place before or behind the *Description* column so you can read them side-by-side.
5. Click **OK**.

Even if you don't add the column, the Netmon filter will work. But your troubleshooting will be much easier if you can see what stage of authentication you're in.

When looking for instances of Proxy Authentication, be sure to study all frames where there is an NTLM Challenge, or an Authenticate Message is present. If necessary, right-click the specific piece of traffic and Find Conversations > TCP. Be aware of the Time Delta values in these Conversations.

Frame Summary - [Conversation Filter]						
Find   						
Frame Number	Time Date Local Adjusted	Time Offset	Time Delta	Process Name	NTLMSSP Summary	Conv Id
2943	9:14:02 AM 2/27/2015	16.9582094	0.0000000	outlook.exe		{TCP:468, IPv4:467}
2948	9:14:02 AM 2/27/2015	17.0323365	0.0741271	outlook.exe		{TCP:468, IPv4:467}
2949	9:14:02 AM 2/27/2015	17.0330259	0.0006894	outlook.exe		{TCP:468, IPv4:467}
2950	9:14:02 AM 2/27/2015	17.0337605	0.0007346	outlook.exe	NTLM NEGOTIATE MESSAGE, Workstation N...	{HTTP:472, TCP:468, IPv4:467}
2955	9:14:02 AM 2/27/2015	17.1084402	0.0746797	outlook.exe		{TCP:468, IPv4:467}
2956	9:14:02 AM 2/27/2015	17.1167295	0.0082893	outlook.exe	NTLM CHALLENGE MESSAGE	{HTTP:472, TCP:468, IPv4:467}
2957	9:14:02 AM 2/27/2015	17.1167809	0.0000514	outlook.exe		{TCP:468, IPv4:467}
2958	9:14:02 AM 2/27/2015	17.1192755	0.0024946	outlook.exe	NTLM AUTHENTICATE MESSAGEVersion:v2, ...	{HTTP:472, TCP:468, IPv4:467}

A four second delay in proxy authentication as seen in Wireshark. The **Time delta from previous displayed frame** column was made via right-clicking the field of the same name in the frame details and selecting Add as Column.

Time	Source	Time delta from previous displayed frame	Destination	Protocol	Info
9 0.127317300	10.190.224.120	0.000390100	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
10 0.127317300	10.190.224.120	0.000000000	10.164.114.89	HTTP	HTTP/1.1 407 Proxy Authentication Required (Forefront TMG requires authorization
11 0.127354100	10.164.114.89	0.000036800	10.190.224.120	TCP	60299-8080 [ACK] Seq=565 Ack=4556 win=262144 Len=0
12 0.251045900	10.164.114.89	0.123691800	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
13 0.251045900	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
14 0.251045900	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
15 0.251045900	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
16 0.251797400	10.190.224.120	0.000751500	10.164.114.89	TCP	8080-60299 [ACK] Seq=4556 Ack=6405 win=131328 Len=0
17 0.251837200	10.164.114.89	0.000039800	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
18 0.251837200	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
19 0.251837200	10.164.114.89	0.000000000	10.190.224.120	TCP	[TCP segment of a reassembled PDU]
20 0.251837200	10.164.114.89	0.000000000	10.190.224.120	HTTP	GET http://www.bing.com/ HTTP/1.1
21 0.252528000	10.190.224.120	0.000690800	10.164.114.89	TCP	8080-60299 [ACK] Seq=4556 Ack=9325 win=131328 Len=0
22 0.252528000	10.190.224.120	0.000000000	10.164.114.89	TCP	8080-60299 [ACK] Seq=4556 Ack=10842 win=131328 Len=0
23 4.220500000	10.190.224.120	3.967972000	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
24 4.220579100	10.164.114.89	0.000079100	10.190.224.120	TCP	60299-8080 [ACK] Seq=10842 Ack=5254 win=261376 Len=0
25 4.361238800	10.190.224.120	0.140659700	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
26 4.361317500	10.164.114.89	0.000078700	10.190.224.120	TCP	60299-8080 [ACK] Seq=10842 Ack=6714 win=262144 Len=0
27 4.361383400	10.190.224.120	0.000065900	10.164.114.89	TCP	[TCP segment of a reassembled PDU]
28 4.361383400	10.190.224.120	0.000000000	10.164.114.89	TCP	[TCP segment of a reassembled PDU]

DNS Performance

Name resolution works best and most quickly when it takes place as close to the client's country as possible.

If DNS name resolution is taking place overseas, it can add seconds to page loads. Ideally, name resolution happens in under 100ms. If not, you should do further investigation.

TIP

Not sure how Client Connectivity works in Office 365? Take a look at the Client Connectivity Reference document [here](#).

Tools

- Netmon
- Wireshark
- PsPing

What to look for

Analyzing DNS performance is typically another job for a network trace. However, PsPing is also helpful in ruling in, or out, a possible cause.

DNS traffic is based on TCP and UDP requests and responses are clearly marked with an ID that will help to match a specific request with its specific response. You'll see DNS traffic when, for example, SharePoint Online uses a network name or URL on a web page. As a rule of thumb, most of this traffic, except when transferring Zones, runs over UDP.

In both Netmon and Wireshark, the most basic filter that will let you look at DNS traffic is simply `dns`. Be sure to use lower case when specifying the filter. Remember to flush your DNS resolver cache before you begin to reproduce the issue on your client computer. For example, if you have a slow SharePoint Online page load for the Home page, you should close all browsers, open a new browser, start tracing, flush your DNS resolver cache, and browse to your SharePoint Online site. Once the entire page resolves, you should stop and save the trace.

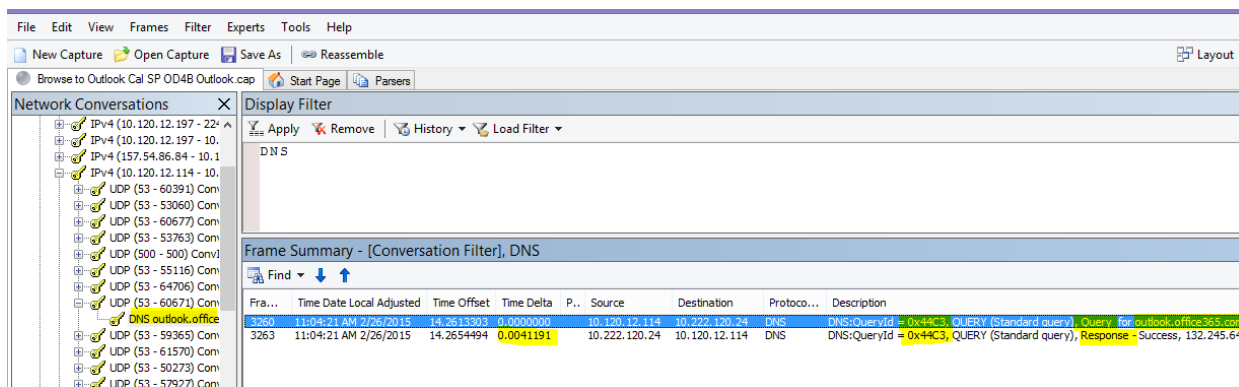
Display Filter						
Apply Remove History Load Filter						
DNS						
Frame Summary - DNS						
Find Find Find						
Cal Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
/25/2015	14.7454102		10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0x6153, QUERY (Standard query), Response - Success,
/25/2015	15.0606288		10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0xC582, QUERY (Standard query), Query for prod.msocdn.com of type AAAA on das
/25/2015	15.0646496		10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0xC582, QUERY (Standard query), Response - Success, 2600:1409:A:388:0:0:0:1D8E
/25/2015	15.2505381		10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0xE69, QUERY (Standard query), Query for outlook.office365.com of type Host Addr
/25/2015	15.2508051		10.120.12.114	10.222.120.24	DNS	DNS:QueryId = 0x5B08, QUERY (Standard query), Query for outlook.office365.com of type AAAA on
/25/2015	15.2544294		10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0xE69, QUERY (Standard query), Response - Success, 132.245.81.146, 157.56.239.1
/25/2015	15.2560364		10.222.120.24	10.120.12.114	DNS	DNS:QueryId = 0x5B08, QUERY (Standard query), Response - Success, 2A01:111:F400:2C2C:0:0:0:2

You want to look at the time offset here. And it may be helpful to add the **Time Delta** column to Netmon which you can do by completing these steps:

1. Right-click on a column such as **Description**.
2. Click **Choose Columns**.

3. Locate *Time Delta* in the list and click **Add**.
4. Move the new column into place before or behind the *Description* column so you can read them side-by-side.
5. Click **OK**.

If you find a query of interest, consider isolating it by right-clicking that query in the frame details panel, choosing **Find Conversations > DNS**. Notice that the Network Conversations panel jumps right to the specific conversation in its log of UDP traffic.



In Wireshark you can make a column for DNS time. Take your trace (or open a trace) in Wireshark and filter by `dns`, or, more helpfully, `dns.time`. Click on any DNS query, and, in the panel showing details, expand the `Domain Name System (response)` details. You'll see a field for time (for example, `[Time: 0.001111100 seconds]`). Right-click this time and select **Apply as Column**. This will give you a **Time** column for quicker sorting of your trace. Click on the new column to sort by descending values to see which DNS call took the longest to resolve.

[A browse of SharePoint Online filtered in Wireshark by \(lowercase\) dns.time, with the time from the details made into a column and sorted ascending.](#)

If you would like to do more investigation of the DNS resolution time, try a PsPing against the DNS port used by TCP (for example, `psping <IP address of DNS server>:53`). Do you still see a performance issue? If you do, then the problem is more likely to be a broader network issue than an issue of specific the DNS application you're hitting to do resolution. It's also worth mentioning, again, that a ping to outlook.office365.com will tell you where DNS name resolution for Outlook Online is taking place (for example, outlook-namnorthwest.office365.com).

If the issue looks to be DNS specific, it may be necessary to contact your IT department to look at DNS configurations and DNS Forwarders to further investigate this issue.

Proxy Scalability

Services like Outlook Online in Office 365 grant clients multiple long-term connections. Therefore, each user may use more connections that require a longer life.

Tools

Math

What to look for

There is no network trace or troubleshooting tool specific to this. Instead, it's based upon bandwidth calculations given limitations and other variables.

TCP Max Segment Size

Found in the SYN - SYN/ACK. Do this check in any performance network trace you've taken to ensure that TCP packets are configured to carry the maximum amount of data possible.

The goal is to see an MSS of 1460 bytes for transmission of data. If you're behind a proxy, or you are using a NAT, remember to run this test from client to proxy/egress/NAT, and from proxy/egress/NAT to Office 365 for

best results! These are different TCP sessions.

Tools

Netmon

What to look for

TCP Max Segment Size (MSS) is another parameter of the three-way handshake in your network trace, that means you'll find the data you need in the SYN - SYN/ACK packet. MSS is actually pretty simple to see.

Open any performance network trace you have and find the connection you're curious about, or that demonstrates the performance problem.

NOTE

If you are looking at a trace and need to find the traffic relevant to your conversation, filter by the IP of the Client, or the IP of the proxy server or egress point, or both. Going directly, you will need to ping the URL that you're testing for the IP address of Office 365 in the trace, and filter by it.

Looking at the trace second-hand? Try using filters to orient yourself. In Netmon, run a search based on the URL, such as `Containsbin(framedata, ascii, "sphybridExample")`, take note of the frame number.

In Wireshark use something like `frame contains "sphybridExample"`. If you notice that you've found Remote Winsock (RWS) traffic (it may appear as a [PSH, ACK] in Wireshark), remember that RWS connects can be seen shortly before relevant SYN - SYN/ACKs, as discussed earlier.

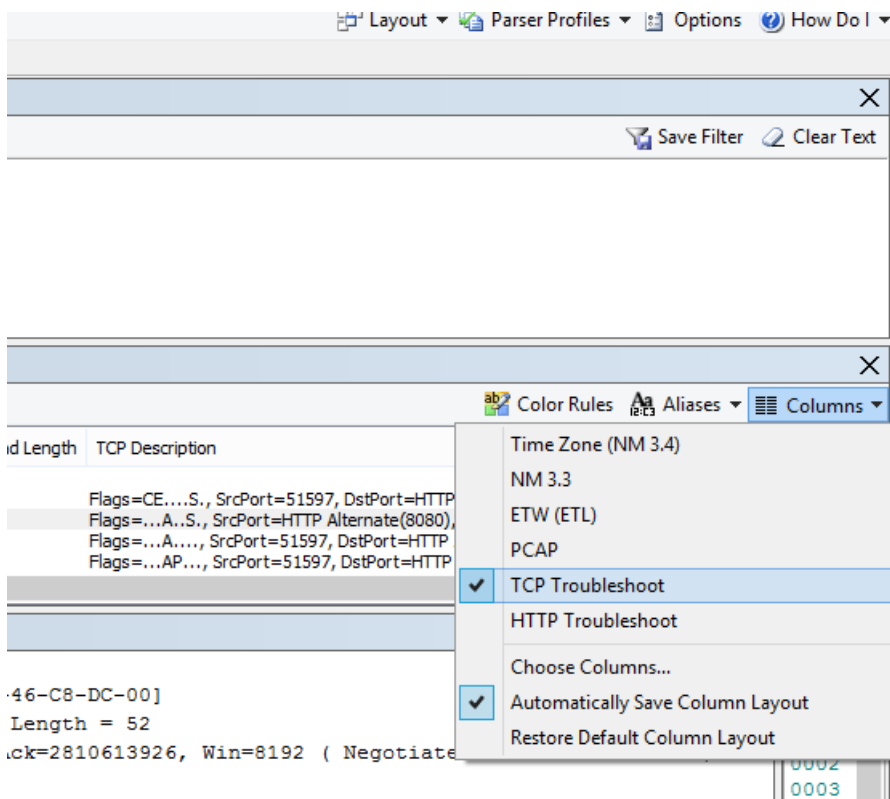
At this point, you can record the frame number, drop the filter, click **All Traffic** in the Network Conversations window in Netmon to look at the nearest SYN.

Importantly, if you didn't receive any of the IP address information at the time of the trace, finding your URL in the trace (part of `sphybridExample-my.sharepoint.com`, for example), will give you IP addresses to filter by.

Locate the connection in the trace that you're interested in seeing. You may do this by either scanning the trace, by filtering by IP addresses, or by selecting specific Conversation IDs using the Network Conversations window in Netmon. Once you've found the SYN packet, expand TCP (in Netmon), or Transmission Control Protocol (in Wireshark) in the Frame Details panel. Expand TCP Options and MaxSegmentSize. Locate the related SYN-ACK frame and Expand TCP Options and MaxSegmentSize. The smaller of the two values will be your Maximum Segment Size. In this picture, I make use of the built-in Column in Netmon called TCP Troubleshoot.

Frame Summary									
Find ↓ ↑ Color Rule									
Frame Number	Time Delta	Source	Destination	TCP Short Sequence Range	TCP Short Ack Number	TCP Fl...	TCP Window Size	TCP Payload Length	TCP Description
1	0.0000000								
2	0.0000000	10.164.114.89	10.190.224.84	0	0 (0x0)	CE...S.	65535	0	Flags=CE...S., SrcPort=51597, DstPort=HTTP Alternate(8080)
3	0.2598509	10.190.224.84	10.164.114.89	0	1	...A..S.	2097152	0	Flags=...A..S., SrcPort=HTTP Alternate(8080), DstPort=51597
4	0.0008366	10.164.114.89	10.190.224.84	1	1	...A....	262144	0	Flags=...A...., SrcPort=51597, DstPort=HTTP Alternate(8080)
5	0.0005668	10.164.114.89	10.190.224.84	1 - 248	1	...AP...	262144	247	Flags=...AP..., SrcPort=51597, DstPort=HTTP Alternate(8080)
<									
Frame Details									
Frame: Number = 3, Captured Frame Length = 66, MediaType = ETHERNET									
Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-18-FE-62-EE-F2], SourceAddress: [00-1D-46-C8-DC-00]									
IPv4: Src = 10.190.224.84, Dest = 10.164.114.89, Next Protocol = TCP, Packet ID = 1999, Total IP Length = 52									
TCP: Flags=...A..S., SrcPort=HTTP Alternate(8080), DstPort=51597, PayloadLen=0, Seq=2729334249, Ack=2810613926, Win=8192 (Negotiated scale fa									
- SrcPort: HTTP Alternate(8080)									
- DstPort: 51597									
- SequenceNumber: 2729334249 (0xA2AE55E9)									
- AcknowledgementNumber: 2810613926 (0xA78690A6)									
- DataOffset: 128 (0x80)									
- Flags: ...A..S.									
- Window: 8192 (Negotiated scale factor 0x8) = 2097152									
- Checksum: 0xCD0D, Good									
- UrgentPointer: 0 (0x0)									
- TCPOptions:									
- MaxSegmentSize: 1									
- type: Maximum Segment Size. 2 (0x2)									
- OptionLength: 4 (0x4)									
- MaxSegmentSize: 1460 (0x5B4)									

The built-in column is at the top of the **Frame Details** panel. (To switch back to your normal view, click **Columns** again, and then choose **Time Zone**.)



Here's a filtered trace in Wireshark. There is a filter specific to the MSS value (`tcp.options.mss`). The frames of a SYN, SYN/ACK, ACK handshake are linked at the bottom of the Wireshark equivalent to Frame Details (so frame 47 ACK, links to 46 SYN/ACK, links to 43 SYN) to make this kind of work easier.

No.	Time	Source	Destination	Protocol	Time	Info
42	0.038290000	10.120.12.114	157.54.86.84	TCP		5809->1/43 [PSH, ACK] Seq=303 Ack=771 Win=232 Len=261
43	0.039039500	10.120.12.114	157.54.86.84	TCP		58100->40700 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SA
44	0.039887500	157.54.86.84	10.120.12.114	TCP		1745->58097 [PSH, ACK] Seq=771 Ack=844 win=255 Len=281
45	0.040505800	10.120.12.114	157.54.86.84	TCP		58099->40702 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SA
46	0.080978100	157.54.86.84	10.120.12.114	TCP		40700->58100 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460
47	0.081497400	10.120.12.114	157.54.86.84	TCP		58100->40700 [ACK] Seq=1 Ack=1 win=262144 Len=0
48	0.082292500	157.54.86.84	10.120.12.114	TCP		40702->58099 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460
49	0.082619100	10.120.12.114	157.54.86.84	TCP		58099->40702 [ACK] Seq=1 Ack=1 win=262144 Len=0

[Destination GeoIP: unknown]	
Transmission Control Protocol, Src Port: 40700 (40700), Dst Port: 58100 (58100), Seq: 0, Ack: 1, Len: 0	
Source Port: 40700 (40700)	
Destination Port: 58100 (58100)	
[Stream index: 1]	
[TCP segment Len: 0]	
Sequence number: 0 (relative sequence number)	
Acknowledgment number: 1 (relative ack number)	
Header Length: 32 bytes	
... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)	
window size value: 4380	
[calculated window size: 4380]	
Checksum: 0x806d [validation disabled]	
urgent pointer: 0	
Options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, SACK permitted, End of option List (EOL)	
Maximum segment size: 1460 bytes	
Kind: Maximum segment size (2)	
Length: 4	
MSS value: 1460	
No-operation (NOP)	
Window scale: 2 (multiply by 4)	
TCP SACK Permitted Option: True	
End of Option List (EOL)	
[SEQ/ACK analysis]	
This is an ACK to the segment in frame: 43	
[The RTT to ACK the segment was: 0.041938600 seconds]	
[RTT: 0.042457900 seconds]	

If you need to check **Selective Acknowledgment** (next topic in this matrix), don't close your trace!

Selective Acknowledgment

Found in the SYN - SYN/ACK. Must be reported as Permitted in both SYN and SYN/ACK. Selective Acknowledgment (SACK) allows for smoother retransmission of data when a packet or packets go missing. Devices can disable this feature, which can lead to performance problems.

If you're behind a proxy, or you are using a NAT, remember to run this test from client to proxy/egress/NAT, and from proxy/egress/NAT to Office 365 for best results! These are different TCP sessions.

Tools

Netmon

What to look for

Selective Acknowledgment (SACK) is another parameter in the SYN-SYN/ACK handshake. You can filter your trace for SYN - SYN/ACK many ways.

Locate the connection in the trace that you're interested in seeing either by scanning the trace, filtering by IP addresses, or by clicking a Conversation ID using the Network Conversations window in Netmon. Once you've found the SYN packet, expand TCP in Netmon, or Transmission Control Protocol in Wireshark in the Frame Details section. Expand TCP Options and then SACK. Locate the related SYN-ACK frame and Expand TCP Options and its SACK field. Make certain SACK is permitted in both SYN and SYN/ACK. Here are SACK values as seen in both Netmon and Wireshark.

Display Filter

Apply Remove History Load Filter

tcp.Flags.Syn == 1

Frame Summary - tcp.Flags.Syn == 1

Frame Number	Time Date Local Adjusted	Time Offset	Time Delta	Process Name	Source	Destination	Protocol Name	Description
2	12:16:32 PM 3/4/2015	0.0000000	0.0000000	IEXPLORE.EXE	10.164.114.89	10.190.224.84	TCP	TCP:Flags=CE...S., SrcPort=51597, DstPort=HT
3	12:16:32 PM 3/4/2015	0.2598509	0.2598509	IEXPLORE.EXE	10.190.224.84	10.164.114.89	TCP	TCP:Flags=...A..S., SrcPort=HTTP Alternate(808

Frame Details

- Frame: Number = 2, Captured Frame Length = 66, MediaType = ETHERNET
 - + Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-1D-46-C8-DC-00], SourceAddress:[00-18-FE-62-EE-F2]
 - + Ipv4: Src = 10.164.114.89, Dest = 10.190.224.84, Next Protocol = TCP, Packet ID = 12234, Total IP Length = 52
 - + Tcp: Flags=CE...S., SrcPort=51597, DstPort=HTTP Alternate(8080), PayloadLen=0, Seq=2810613925, Ack=0, Win=65535
 - SrcPort: 51597
 - DstPort: HTTP Alternate(8080)
 - SequenceNumber: 2810613925 (0xA78690A5)
 - AcknowledgementNumber: 0 (0x0)
 - + DataOffset: 128 (0x80)
 - + Flags: CE....S.
 - Window: 65535 (Negotiating scale factor 0x8) = 65535
 - Checksum: 0xE4F6, Good
 - UrgentPointer: 0 (0x0)
 - + TCPOptions:
 - + MaxSegmentSize: 1
 - type: Maximum Segment Size. 2 (0x2)
 - OptionLength: 4 (0x4)
 - MaxSegmentSize: 1460 (0x5B4)
 - + NoOption:
 - + WindowsScaleFactor: ShiftCount: 8
 - + NoOption:
 - + NoOption:
 - + SACKPermitted:
 - type: SACK permitted. 4 (0x4)
 - OptionLength: 2 (0x2)

Filter: tcp.flags.syn == 1

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Time	Info
1	0.000000000	10.164.114.89	10.190.224.120	TCP		51387→8080 [SYN, ECN, CWR] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.005432300	10.190.224.120	10.164.114.89	TCP		8080→51387 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
80	0.356032500	10.164.114.89	10.190.224.120	TCP		51388→8080 [SYN, ECN, CWR] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
81	0.360118200	10.190.224.120	10.164.114.89	TCP		8080→51388 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
101	0.432370500	10.164.114.89	10.190.224.120	TCP		51390→8080 [SYN, ECN, CWR] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: Cisco_c8:dc:00 (00:1d:46:c8:dc:00), Dst: Hewlett-_62:ee:f2 (00:18:fe:62:ee:f2)

Internet Protocol Version 4, Src: 10.190.224.120 (10.190.224.120), Dst: 10.164.114.89 (10.164.114.89)

Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 51387 (51387), Seq: 0, Ack: 1, Len: 0

Source Port: 8080 (8080)

Destination Port: 51387 (51387)

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

Header Length: 32 bytes

... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)

window size value: 8192

[calculated window size: 8192]

checksum: 0xcc6d [validation disabled]

Urgent pointer: 0

options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, No-operation (NOP), No-operation (NOP), SACK permitted

Maximum segment size: 1460 bytes

Kind: Maximum Segment Size (2)

Length: 4

MSS Value: 1460

No-operation (NOP)

Window scale: 8 (multiply by 256)

No-operation (NOP)

No-operation (NOP)

TCP SACK Permitted Option: True

Kind: SACK Permitted (4)

Length: 2

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 1]

[The RTT to ACK the segment was: 0.005432300 seconds]

[RTT: 0.005982300 seconds]

DNS Geolocation

Where in the world Office 365 tries to resolve your DNS call affects your connection speed.

In Outlook Online, after the first DNS lookup is completed, the location of that DNS will be used to connect to your nearest datacenter. You will be connected to an Outlook Online CAS server, which will use the backbone network to connect to the datacenter (dC) where your data is stored. This is faster.

When accessing SharePoint Online, a user traveling abroad will be directed to their active datacenter -- that's the dC whose location is based on their SPO tenant's home-base (so, a dC in the USA if the user is USA-based).

Lync online has active nodes in more than one dC at a time. When requests are sent for Lync online instances, Microsoft's DNS will determine where in the world the request came from, and return IP addresses from the nearest regional dC where Lync online is active.

TIP

Need to know more about how clients connect to Office 365? Take a look at the [Client Connectivity](#) reference article (and its helpful graphics).

Tools

- Ping
- PsPing

What to look for

Requests for name resolution from the client's DNS servers to Microsoft's DNS servers should in most cases result in Microsoft DNS returning the IP address of a regional datacenter (dC). What does this mean for you? If your headquarters are in Bangalore, India, but you are traveling in the United States, when your browser makes a request for Outlook Online, Microsoft's DNS servers should hand you IP addresses to datacenters in the United States -- a regional datacenter. If mail is needed from Outlook, that data will travel across Microsoft's quick backbone network between the datacenters.

DNS works fastest when name resolution is done as close to the user location as possible. If you're in Europe, you want to go to a Microsoft DNS in Europe, and (ideally) deal with a datacenter in Europe. Performance from a client in Europe going to DNS and a datacenter in America will be slower.

Run the Ping tool against outlook.office365.com to determine where in the world your DNS request is being

routed. If you are in Europe, you should see a reply from something like outlook-emeawest.office365.com. In the Americas, expect something like outlook-namnorthwest.office365.com.

Open the command prompt on the client computer (via Start > Run > cmd or Windows key > type cmd). Type ping outlook.office365.com and press ENTER. Remember, to specify -4 if you want to specify to ping via IPv4. You may fail to get a reply from the ICMP packets, but you should see the name of the DNS to which the request was routed. If you want to see the latency numbers for this connection try PsPing to the IP address of the server that is returned by ping.

```
C:\Perf>ping outlook.office365.com

Pinging outlook-namnorthwest.office365.com [132.245.64.146] with 32 bytes of data:
Reply from 132.245.64.146: bytes=32 time=28ms TTL=240
Reply from 132.245.64.146: bytes=32 time=28ms TTL=240
Reply from 132.245.64.146: bytes=32 time=28ms TTL=240
Reply from 132.245.64.146: bytes=32 time=28ms TTL=240

Ping statistics for 132.245.64.146:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 28ms, Average = 28ms
```

```
C:\Perf>psping 132.245.64.146:443

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 132.245.64.146:443:
5 iterations (warmup 1) connecting test:
Connecting to 132.245.64.146:443 (warmup): 28.75ms
Connecting to 132.245.64.146:443: 30.10ms
Connecting to 132.245.64.146:443: 31.31ms
Connecting to 132.245.64.146:443: 29.63ms
Connecting to 132.245.64.146:443: 30.15ms

TCP connect statistics for 132.245.64.146:443:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Minimum = 29.63ms, Maximum = 31.31ms, Average = 30.30ms
```

Office 365 Application Troubleshooting

Tools

- Netmon
- HTTPWatch
- F12 Console in the browser

We don't cover tools used in application-specific troubleshooting in this network-specific article. But you'll find resources you *can* use [on this page](#).

Related Topics

[Managing Office 365 endpoints](#)

[Office 365 endpoints FAQ](#)

Device management roadmap for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

Microsoft 365 for enterprise includes features to help manage devices, and their apps, within your organization. Managing mobile devices helps you secure and protect your organization's resources.

There are two options for device management:

- [Microsoft Intune](#)
- [Basic Mobility and Security](#)

Microsoft Intune

You can use Microsoft Intune to manage access to your organization using mobile device management or mobile application management. Mobile device management is when users "enroll" their devices in Intune. After a device is enrolled, it is a managed device; therefore, it can receive your organization's policies, rules, and settings. For example, you can install specific apps, create a password policy, install a VPN connection, and more.

Users with their own personal devices may not want to enroll their devices or be managed by Intune and your organization's policies. But you still need to protect your organization's resources and data. In this scenario, you can protect your apps using mobile application management. For example, you can use a mobile application management policy that requires a user to enter a PIN when accessing SharePoint Online on the device.

You'll also determine how you're going to manage personal devices and organization-owned devices. You might want to treat devices differently, depending on their uses.

Basic Mobility and Security

This is built into Microsoft 365 and helps you secure and manage your users' mobile devices like iPhones, iPads, Androids, and Windows phones. You can create and manage device security policies, remotely wipe a device, and view detailed device reports.

Choose between the two options

To help you better assess which device management option is best for you, see [Choose between Basic Mobility Security and Intune](#).

Based on your assessment, get started managing your devices with:

- [Intune](#)
- [Basic Mobility and Security](#)

Identity and device access recommendations

Microsoft provides a set of recommendations for [identity and device access](#) to ensure a secure and productive workforce. For device access, use the recommendations and settings in these articles:

- [Prerequisites](#)
- [Common identity and device access policies](#)

How Contoso did device management for Microsoft 365

For information about how a fictional but representative multi-national business deployed their mobile device management infrastructure with Microsoft 365 cloud services, see [Mobile device management for Contoso](#).

Deployment and update channel example configurations

10/28/2022 • 2 minutes to read • [Edit Online](#)

Choosing which update channels to use for Windows 10 and Microsoft 365 Apps can depend on your type of organization and where on the development cycle you want to be deploying and using new features and capabilities. Find the pre-release and production channels that best fit your needs.

Pre-release channels

CUSTOMER/CHANNEL OFFERING	WINDOWS 10	MICROSOFT 365 APPS FOR ENTERPRISE (WINDOWS 10)
Right for highly technical users and developers. Be the first to access the latest builds earliest in the development cycle with the newest code. There will be rough edges and some instability.	Dev	N/A
Right for early adopters and IT Pros who want more reliable builds that are still in development. See what's coming up next and help validate new features.	Beta Channel	Beta Channel
Right for those who want early access to upcoming releases. Where companies preview and validate upcoming releases before broad deployment. These are supported.	Release Preview	Current Channel (Preview) Semi-Annual Enterprise Channel (Preview)

Production channels for broad deployment

Click the link in the **Example** column to step through deployment stages and groups for an example organization.

CUSTOMER/CHANNEL OFFERING	WINDOWS 10	MICROSOFT 365 APPS FOR ENTERPRISE (WINDOWS 10)	EXAMPLE
Right for customers who want the latest releases as soon as they're ready.	Semi-Annual Channel	Current Channel	Latest releases

CUSTOMER/CHANNEL OFFERING	WINDOWS 10	MICROSOFT 365 APPS FOR ENTERPRISE (WINDOWS 10)	EXAMPLE
Right for enterprises who want the latest release with more predictability.	Semi-Annual Channel	Monthly Enterprise Channel	
Right for enterprises with need for extensive IT testing before each update.	Semi-Annual Channel	Semi-Annual Enterprise Channel	

See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Example of broad deployment for the latest releases

10/28/2022 • 4 minutes to read • [Edit Online](#)

This channel configuration example is for an organization that uses rapid deployment of the latest releases to fit these business priorities:

- Ensure business continuity with Microsoft apps and services.
- Maximize device, service, and data security with the latest features and fixes from Microsoft.
- Maximize user productivity with the latest features from Microsoft.

These goals translate to the IT task of finding the balance between rapid production deployment and early vetting with a representative subset of users and devices to validate functionally before broad deployment.

Our example organization has 5,000 employees in buildings across the world in Europe, Africa, Asia, and the Americas. 70% of the employees use Microsoft 365 E3 and the rest of the organization uses Microsoft 365 E5.

NOTE

This example is designed to show you how you can use deployment stages and groups, which can work for organizations of many types and sizes.

This organization's IT infrastructure:

- Is largely homogeneous, with Windows, Microsoft 365 Apps, and Microsoft cloud services comprising 60% of the installed base. A few legacy systems remain after an intensive, multi-year effort to simplify and streamline the IT infrastructure.
- Is maintained by highly experienced staff and tasked with keeping users and their devices productive and secure by following Microsoft's lead in their releases.

Deployment and update stages

Based on rapid deployment goals of the latest release, this example organization uses a two-step deployment process.

1. **Use a preview or pilot deployment:** Validate and iterate with early adopters, IT staff, users with representative configurations, and training staff.

The early adopters, IT staff, users with representative configurations can validate functionality with other apps and on devices before the new features roll out to the rest of the organization.

Change managers have an early peek at the new features before widespread rollout and can plan messaging and rollout.

Training staff can plan new internal courses or update existing courses for the new features before widespread rollout.

2. **Production deployment:** Roll out to all remaining users by region, department, or other deployment method.

Deployment configuration for Windows 10

The overall goal is to perform a broad deployment of the latest Semi-Annual Channel release after validation of

Release Preview Channel changes by a group of representative users and their devices.

See [Windows 10 deployment](#) for more information on Windows 10 deployment methods and strategies.

STAGE	CHANNEL	DEPLOYMENT GROUP
Pilot	Release Preview Channel • Purpose: Deployment of feature updates to IT staff and early adopters for validation on representative devices and configurations (languages, 3rd party apps). • State: Fully compliant and supported for commercial customers and it doesn't count against your support agreements.	Win10ReleasePreviewChannel (example name) Members are groups containing: • Windows enthusiasts across departments and locations • Staff with configurations that need validation • IT admins and IT deployment staff • Change managers • Internal training staff
Production	Semi-Annual Channel • Purpose: Broad deployment of the latest feature updates to the rest of the organization. • State: Fully compliant and supported.	Win10SemiAnnualChannel (example name) Members are all users that aren't in the Win10ReleasePreviewChannel group.

This organization uses the best practice of deploying the Release Preview Channel payload in the same way as they deploy Semi-Annual Channel releases, such as Windows Update or Windows Server Update Services, and that they apply the same policies for both channel updates.

Ongoing updates process:

1. Release Preview Channel changes are deployed to the Win10ReleasePreviewChannel (example name) deployment group.
2. Win10ReleasePreviewChannel group members confirm that Release Preview Channel changes are working to IT deployment staff, who can provide feedback to Microsoft and wait for the next Release Preview Channel changes for additional validation.
3. Semi-Annual Channel feature changes are deployed to the Win10SemiAnnualChannel deployment group.

NOTE

While the Semi-Annual Channel is the recommended channel, your IT department should utilize their management tools and determine when to deploy the latest Semi-Annual Channel release within their organization and then roll it out in waves.

Deployment configuration for Microsoft 365 Apps

The overall goal is to perform a broad deployment of the latest Current Channel release after validation of Current Channel (Preview) changes by a group of representative users.

See [Microsoft 365 Apps deployment](#) for more information on Microsoft 365 Apps deployment methods and strategies.

STAGE	CHANNEL	DEPLOYMENT GROUP
Pilot	Current Channel (Preview) - Purpose: {give a group of representative users a sneak peek of new Microsoft 365 Apps features} Deployment of feature updates as soon as they're tested with Current Channel (Preview) users and are production-ready. - State: Fully compliant and supported. - How often: Updates 2-3 times each month.	AppsCurrentChannelPreview (example name) Members are groups containing: - Office apps enthusiasts across departments and locations - Staff with configurations that need validation - IT admins and IT deployment staff - Change managers - Internal training staff
Production	Current Channel - Purpose: Broad deployment of the latest feature updates to the rest of the organization. - State: Fully compliant and supported.	AppsCurrentChannel (example name) Members are all users that aren't in the AppsCurrentChannelPreview group.

Ongoing updates process:

1. Current Channel (Preview) changes are deployed to the AppsCurrentChannelPreview deployment group.
2. AppsCurrentChannelPreview group members confirm that Current Channel (Preview) changes are working to IT deployment staff, who can provide feedback to Microsoft and wait for the next Current Channel (Preview) release for additional validation.
3. Current Channel changes are deployed to the AppsCurrentChannel deployment group.

Visual summary

Here are the products, their channels, and the deployment groups used by this example organization.

	Deployment phase	Channel	Deployment group (example names)
Windows 10	Pilot: Test for features and hardware and software compatibility with representative devices.	Release Preview Channel	Win10ReleasePreviewChannel
	Production: Roll out to all other Windows devices.	Semi-Annual Channel	Win10SemiAnnualChannel
Microsoft 365 Apps	Pilot: Test for features and app compatibility with representative users.	Current Channel (Preview)	AppsCurrentChannelPreview
	Production: Roll out to all other users.	Current Channel	AppsCurrentChannel

See also

[Deployment and update channel example configurations](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Manage Microsoft 365 with PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

PowerShell for Microsoft 365 is a powerful management tool that complements the Microsoft 365 admin center. For example, you can use PowerShell automation to easily manage multiple user accounts and licenses and to create reports.

Select from the following topics to learn how to use PowerShell to manage Microsoft 365:

- **Get started**

Start here if you're not familiar with PowerShell for Microsoft 365, and you want to install the Microsoft 365 modules and connect to your subscription.

- **User accounts, licenses, and groups**

Start here if you want to learn about using automation commands to manage user accounts, licenses, and groups.

- **SharePoint**

Start here if you want to use automation commands to manage SharePoint.

- **Exchange Online**

Start here if you want to manage Exchange Online.

- **Email migration**

Start here if you want to migrate your email from pre-existing systems.

- **Security & Compliance Center**

Start here if you want to manage Security & Compliance Center features.

- **Delegated Access Permissions (DAP) partners**

Start here if you want to use Syndication and Cloud Solution Provider (CSP) partners to manage your Microsoft 365 customer tenants.

- **Skype for Business Online**

Start here to manage Skype for Business Online.

Get started with PowerShell for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use commands and scripts in PowerShell for Microsoft 365 to manage Microsoft 365 and streamline your daily work. Use the following information to learn why PowerShell for Microsoft 365 is crucial to managing Microsoft 365, how to connect to your Microsoft 365 subscription and create reports, and where to get more information from the Microsoft 365 community.

Select from these topics:

- [Why you need to use PowerShell for Microsoft 365](#)

Start here if you're new to PowerShell for Microsoft 365. Learn why you should use PowerShell for Microsoft 365.

- [Connect to Microsoft 365 with PowerShell](#)

Start here to connect to your Microsoft 365 subscription by using PowerShell for Microsoft 365 and do administrative tasks from the command line.

- [Connect to all Microsoft 365 services in a single PowerShell window](#)

You can manage Microsoft 365 in separate windows for Skype for Business Online, SharePoint Online, Microsoft Exchange Online, and Microsoft 365 accounts and licenses. Or, you can manage them all from a single window. This article explains how.

- [Use PowerShell to create reports in Microsoft 365](#)

Start here if you've installed the PowerShell for Microsoft 365 modules and want to learn about using automation commands to create reports quickly.

- [Cmdlet references for Microsoft 365 services](#)

Learn about the cmdlets for the PowerShell for Microsoft 365 modules.

- [Microsoft 365 community resources for PowerShell](#)

Start here to connect to the PowerShell community and get more information about using PowerShell for Microsoft 365.

Related topics

[Manage Microsoft 365 with PowerShell](#)

Why you need to use PowerShell for Microsoft 365

10/28/2022 • 17 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

With the Microsoft 365 admin center, you can manage your Microsoft 365 user accounts and licenses. You can also manage your Microsoft 365 services, such as Exchange Online, Teams, and SharePoint Online. If you instead use PowerShell to manage these services, you can take advantage of the command-line and scripting language environment for speed, automation, and additional capabilities.

This article shows how to use PowerShell to manage Microsoft 365 to:

- Reveal additional information that you can't see in the Microsoft 365 admin center
- Configure features and settings only possible with PowerShell
- Do bulk operations
- Filter data
- Print or save data
- Manage across services

Keep in mind that PowerShell for Microsoft 365 is a set of modules for Windows PowerShell, which is a command-line environment for Windows-based services and platforms. This environment creates a command-shell language that can be extended with additional modules. It provides a way to execute simple or complex commands or scripts. For example, after you install the PowerShell for Microsoft 365 modules and connect to your Microsoft 365 subscription, you can run the following command to list all the user mailboxes for Microsoft Exchange Online:

```
Get-Mailbox
```

You could also get the list of mailboxes by using the Microsoft 365 admin center but counting the items in all the lists for all the sites for all of your web apps isn't easy.

PowerShell for Microsoft 365 is designed to help you manage Microsoft 365, not to replace the Microsoft 365 admin center. Admins need to be able to use PowerShell for Microsoft 365 because there are some configuration procedures that can only be done through PowerShell for Microsoft 365 commands. For these cases, you need to know how to:

- Install the PowerShell for Microsoft 365 modules (done only one time for each administrator computer).
- Connect to your Microsoft 365 subscription (one time for each PowerShell session).
- Gather the information needed to run the required PowerShell for Microsoft 365 commands.
- Run PowerShell for Microsoft 365 commands.

After you learn these basic skills, you don't have to list your mailbox users by using the **Get-Mailbox** command. You also don't have to understand how to create a new command like the command cited previously to count all the items in all the lists for all the sites for all of your web apps. Microsoft and the community of administrators can help you with such tasks as needed.

PowerShell for Microsoft 365 can reveal information that you can't see with the Microsoft 365 admin center

The Microsoft 365 admin center displays many useful information. But it doesn't display all the possible information that Microsoft 365 stores about users, licenses, mailboxes, and sites. Here's an example for *users and groups* in the Microsoft 365 admin center:

☐	DISPLAY NAME ^	USER NAME	STATUS
☐	Alex Darrow	AlexD@litwareinc.onmicrosoft.com	In cloud
☐	Allie Bellew	AllieB@litwareinc.onmicrosoft.com	In cloud
☐	Anne Wallace	AnneW@litwareinc.onmicrosoft.com	In cloud
☐	Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	In cloud
☐	Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	In cloud
☐	Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	In cloud
☐	Brian Johnson (TAILSPIN)	BrianJ@litwareinc.onmicrosoft.com	In cloud

This view provides the information that you need in many cases. However, there are times when you need more. For example, Microsoft 365 licensing (and the Microsoft 365 features available to a user) depends in part on the user's geographic location. The policies and features that you can extend to a user who lives in the United States might not be the same as those that you can extend to a user in India or Belgium. Follow these steps in the Microsoft 365 admin center to determine a user's geographic location:

1. Double-click the user's **Display Name**.
2. In the user properties display pane, select **details**.
3. In the details display, select **additional details**.
4. Scroll until you find the heading **Country or region**:

ZIP or postal code:

Country or region:

5. Write the user's display name and location on a piece of paper, or copy and paste it into Notepad.

You must repeat this procedure for each user. If you have many users, this process can be tedious. With PowerShell for Microsoft 365, you can display this information for all of your users by using the following command:

```
Get-AzureADUser | Select DisplayName, UsageLocation
```

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets that have *Mso/* in their name. You have to run these cmdlets from Windows PowerShell.

Here's an example of the results:

DisplayName	UsageLocation
-----	-----
Bonnie Kearney	GB
Fabrice Canel	BR
Brian Johnson (TAILSPIN)	US
Anne Wallace	US
Alex Darrow	US
David Longmuir	BR

The interpretation of this PowerShell command is: Get all of the users in the current Microsoft 365 subscription (**Get-AzureADUser**), but only display the name and location for each user (**Select DisplayName, UsageLocation**).

Because PowerShell for Microsoft 365 supports a command-shell language, you can further manipulate the information obtained by the **Get-AzureADUser** command. For example, maybe you'd like to sort these users by their location, grouping all the Brazilian users together, all the United States users together, and so on. Here's the command:

```
Get-AzureADUser | Select DisplayName, UsageLocation | Sort UsageLocation, DisplayName
```

Here's an example of the results:

DisplayName	UsageLocation
-----	-----
David Longmuir	BR
Fabrice Canel	BR
Bonnie Kearney	GB
Alex Darrow	US
Anne Wallace	US
Brian Johnson (TAILSPIN)	US

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription, but only display the name and location for each user and sort them first by their location and then their name (**Sort UsageLocation, DisplayName**).

You can also use additional filtering. For example, if you only want to see information about users based in Brazil, use this command:

```
Get-AzureADUser | Where {$_.UsageLocation -eq "BR"} | Select DisplayName, UsageLocation
```

Here's an example of the results:

DisplayName	UsageLocation
-----	-----
David Longmuir	BR
Fabrice Canel	BR

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription whose location is Brazil (**Where {\$_.UsageLocation -eq "BR"}**) and then display the name and location for each user.

A note about large domains

If you have a large domain with tens of thousands of users, trying some of the examples we show in this article could lead to throttling. Based on factors like computing power and available network bandwidth, you may be trying to do too much at one time. Large organizations might want to split some of these PowerShell operations into two commands.

For example, the following command returns all the user accounts and shows the name and location for each:

```
Get-AzureADUser | Select DisplayName, UsageLocation
```

That works great for smaller domains. But in a large organization, you might want to split that operation into two commands: one command to store the user account information in a variable and another to display the needed information. Here's an example:

```
$x = Get-AzureADUser  
$x | Select DisplayName, UsageLocation
```

The interpretation of this set of PowerShell commands is:

1. Get all the users in the current Microsoft 365 subscription and store the information in a variable named `$x` (**`$x = Get-AzureADUser`**).
2. Display the contents of the variable `$x`, but only include the name and location for each user (**`$x | Select DisplayName, UsageLocation`**).

Microsoft 365 has features that you can only configure with PowerShell for Microsoft 365

The Microsoft 365 admin center is intended to provide access to common, useful administrative tasks that apply to most environments. In other words, the Microsoft 365 admin center was designed so that the typical administrator can carry out the most-common management tasks. But there are some tasks that can't be done in the admin center.

For example, the Skype for Business Online admin center provides a few options for creating custom meeting invitations:

You can customize Lync meeting invitations to meet your organization's needs. You have one. You can also add legal disclaimers by providing the link to a website with

Logo URL:

Help URL:

Legal URL:

Footer text:

With these settings, you can add a touch of personalization and professionalism to meeting invitations. But there's more to meeting-configuration settings than simply creating custom meeting invitations. For example, by default, meetings allow:

- Anonymous users to gain automatic entrance to each meeting.
- Attendees to record the meeting.
- All users from your organization to be designated as presenters when they join the meeting.

These settings aren't available from the Skype for Business Online admin center. You can control them from PowerShell for Microsoft 365. Here's a command that disables these three settings:

```
Set-CsMeetingConfiguration -AdmitAnonymousUsersByDefault $False -AllowConferenceRecording $False -DesignateAsPresenter "None"
```

NOTE

To run this command, you must install the [Skype for Business Online PowerShell Module](#).

The interpretation of this PowerShell command is:

1. In the settings for new Skype for Business Online meetings (**Set-CsMeetingConfiguration**), disable allowing anonymous users to gain automatic entrance to meetings (**-AdmitAnonymousUsersByDefault \$False**).
2. Disable the ability for attendees to record meetings (**-AllowConferenceRecording \$False**).
3. Don't designate all users from your organization as presenters (**-DesignateAsPresenter "None"**).

To restore these default settings (enable the options), run this command:

```
Set-CsMeetingConfiguration -AdmitAnonymousUsersByDefault $True -AllowConferenceRecording $True -DesignateAsPresenter "Company"
```

There are other similar scenarios as well, which is why administrators should know how to run PowerShell for Microsoft 365 commands.

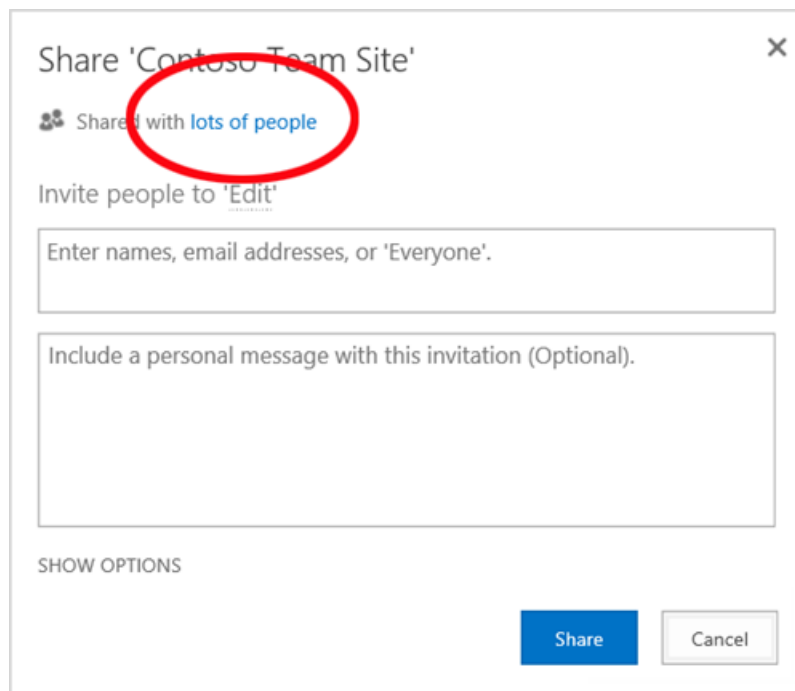
PowerShell for Microsoft 365 is great for bulk operations

Visual interfaces like the Microsoft 365 admin center are most valuable when you have a single operation to do. For example, if you need to disable one user account, you can use the admin center to quickly locate and clear a checkbox. This may be easier than performing a similar operation in PowerShell.

But if you have to change many things or some selected things within a large set of other things, the Microsoft 365 admin center might not be the best tool. For example, say you have to change the prefix on thousands of phone numbers or remove the specific user *Ken Myer* from all your SharePoint Online sites. How would you do that in the Microsoft 365 admin center?

For the last example, say you have several hundred SharePoint Online sites, and you don't know which ones Ken Meyer is a member of. You would have to start at the Microsoft 365 admin center and then perform this procedure for each site:

1. Select the **URL** of the site.
2. In the **site collection properties** box, select the **Web Site Address** link to open the site.
3. On the site, select **Share**.
4. In the **Share** dialog box, select the link that shows all the users who have permissions to the site:



5. In the **Shared With** dialog box, select **Advanced**.
6. Scroll down the list of users, find and select Ken Myer (assuming he has permissions to the site), and then select **Remove User Permissions**.

This would take a *long* time for several hundred sites.

The alternative is to run the following command in PowerShell for Microsoft 365 to remove Ken Myer from all your sites:

```
Get-SPOSite | ForEach {Remove-SPOUser -Site $_.Url -LoginName "kenmyer@litwareinc.com"}
```

NOTE

This command requires that you install the [SharePoint Online PowerShell module](#).

The interpretation of this PowerShell command is: Get all of the SharePoint sites in the current Microsoft 365 subscription (**Get-SPOSite**) and for each site remove Ken Meyer from the list of users who can access it (**ForEach {Remove-SPOUser -Site \$_.Url -LoginName "kenmyer@litwareinc.com"}**).

We tell Microsoft 365 to remove Ken Meyer from every site, including those that he doesn't have access to. So the results will show errors for those sites that he doesn't have access to. We can use an additional condition on this command to remove Ken Meyer only from the sites that have him on their login list. But the errors that are returned cause no harm to the sites themselves. This command might take a few minutes to run against hundreds of sites, rather than hours of working through the Microsoft 365 admin center.

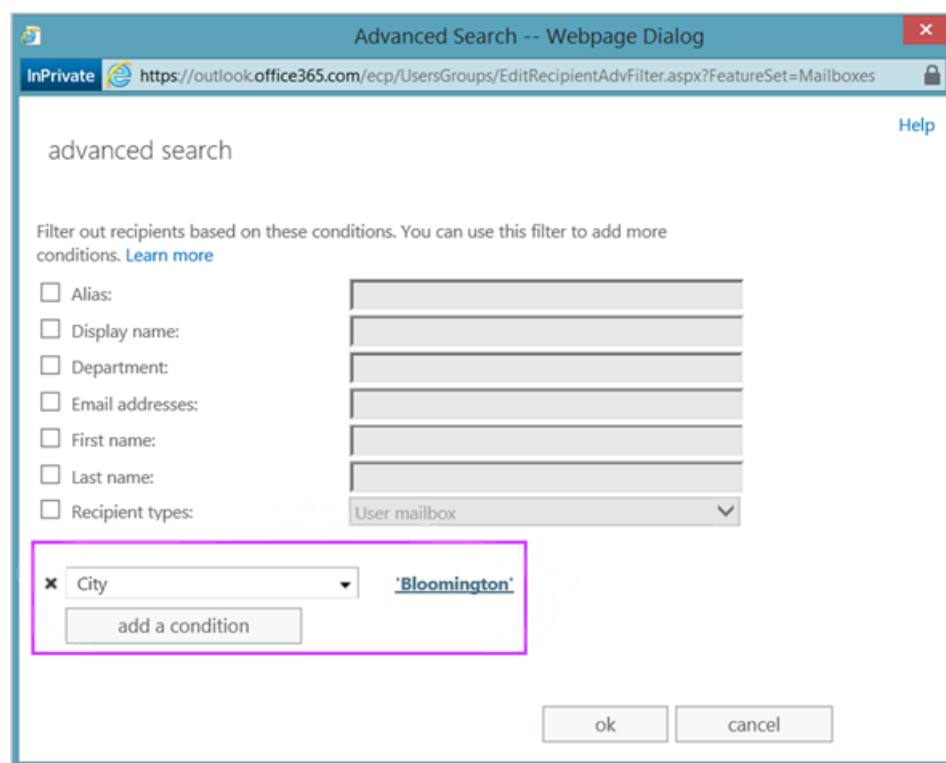
Here's another bulk operation example. Use this command to add *Bonnie Kearney*, a new SharePoint administrator, to all sites in the organization:

```
Get-SPOSite | ForEach {Add-SPOUser -Site $_.Url -LoginName "bkearney@litwareinc.com" -Group "Members"}
```

The interpretation of this PowerShell command is: Get all the SharePoint sites in the current Microsoft 365 subscription and for each site allow Bonnie Kearney access by adding her login name to the Members group of the site (**ForEach {Add-SPOUser -Site \$_.Url -LoginName "bkearney@litwareinc.com" -Group "Members"}**).

PowerShell for Microsoft 365 is great at filtering data

The Microsoft 365 admin center provides several ways to filter your data to easily locate a targeted subset of information. For example, Exchange makes it easy to filter on practically any property of a user mailbox. For example, here's the list of mailboxes for all the users who live in the city of Bloomington:



The [Exchange admin center](#) also lets you combine filter criteria. For example, you can find the mailboxes for all the people who live in Bloomington and work in the Finance department.

But there are limitations to what you can do in the Exchange Admin center. For example, you couldn't as easily find the mailboxes of people who live in Bloomington *or* San Diego, or the mailboxes for all people who don't live in Bloomington.

You can use the following PowerShell for Microsoft 365 command to get a list of mailboxes for all the people who live in Bloomington or San Diego:

```
Get-User | Where {$_.RecipientTypeDetails -eq "UserMailbox" -and ($_.City -eq "San Diego" -or $_.City -eq "Bloomington")) | Select DisplayName, City
```

Here's an example of the results:

DisplayName	City
Alex Darrow	San Diego
Bonnie Kearney	San Diego
Julian Isla	Bloomington
Rob Young	Bloomington

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription who have a mailbox in the city of San Diego or Bloomington (**Where {\$_.RecipientTypeDetails -eq "UserMailbox" -and (\$_.City -eq "San Diego" -or \$_.City -eq "Bloomington"))**), and then display the name and city for each (**Select DisplayName, City**).

And here's the command to list all the mailboxes for people who live anywhere except Bloomington:

```
Get-User | Where {$_.RecipientTypeDetails -eq "UserMailbox" -and $_.City -ne "Bloomington"} | Select DisplayName, City
```

Here's an example of the results:

DisplayName	City
MOD Administrator	Redmond
Alex Darrow	San Diego
Allie Bellew	Bellevue
Anne Wallace	Louisville
Aziz Hassouneh	Cairo
Belinda Newman	Charlotte
Bonnie Kearney	San Diego
David Longmuir	Waukesha
Denis Dehenne	Birmingham
Garret Vargas	Seattle
Garth Fort	Tulsa
Janet Schorr	Bellevue

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription who have a mailbox not located in the city of Bloomington (**Where {\$_.RecipientTypeDetails -eq "UserMailbox" -and \$_.City -ne "Bloomington"}**), and then display the name and city for each.

Use wildcards

You can also use wildcard characters in your PowerShell filters to match part of a name. For example, suppose you're looking for a user account. All you can remember is that the user's last name was *Anderson* or maybe *Henderson* or *Jorgenson*.

You could track down that user in the Microsoft 365 admin center by using the search tool and carrying out three different searches:

- One for *Anderson*
- One for *Henderson*
- One for *Jorgenson*

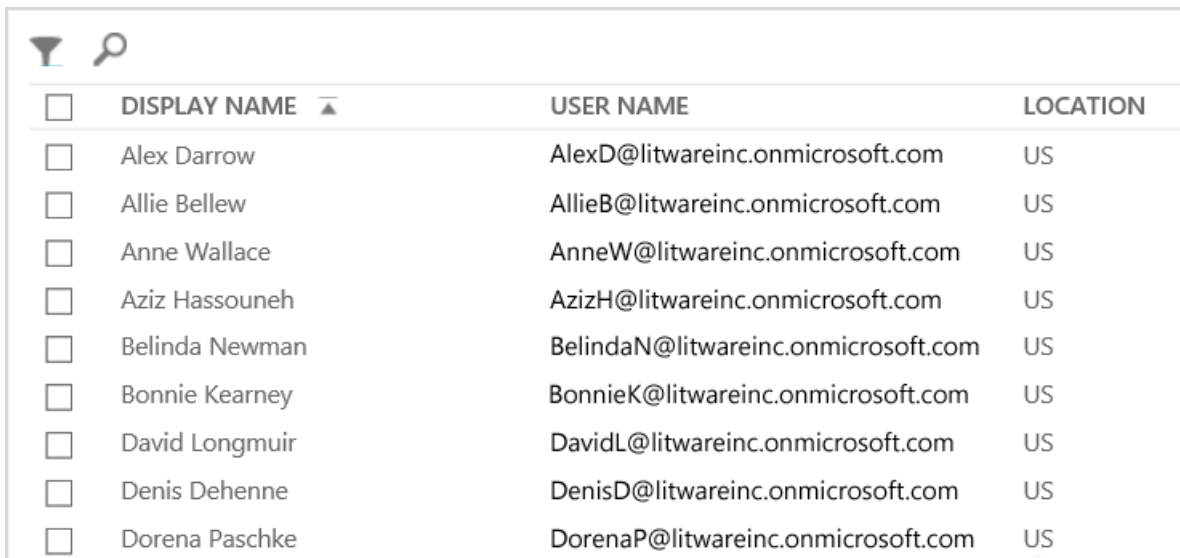
Because all three of these names end in "son", you can tell PowerShell to display all the users whose name ends in "son". Here's the command:

```
Get-User -Filter '{LastName -like "*son"}'
```

The interpretation of this PowerShell command is: Get all the users in the current Microsoft 365 subscription, but use a filter that only lists the users whose last names end in "son" (-Filter '{LastName -like "*son"}'). The * stands for any set of characters, which are letters in the user's last name.

PowerShell for Microsoft 365 makes it easy to print or save data

The Microsoft 365 admin center lets you view lists of data. Here's an example of the Skype for Business Online admin center displaying a list of users who have been enabled for Skype for Business Online:



☐	DISPLAY NAME	USER NAME	LOCATION
☐	Alex Darrow	AlexD@litwareinc.onmicrosoft.com	US
☐	Allie Bellew	AllieB@litwareinc.onmicrosoft.com	US
☐	Anne Wallace	AnneW@litwareinc.onmicrosoft.com	US
☐	Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	US
☐	Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	US
☐	Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	US
☐	David Longmuir	DavidL@litwareinc.onmicrosoft.com	US
☐	Denis Dehenne	DenisD@litwareinc.onmicrosoft.com	US
☐	Dorena Paschke	DorenaP@litwareinc.onmicrosoft.com	US

To save that information to a file, you must paste it into a document or Microsoft Excel worksheet. Either case might require additional formatting. Additionally, the Microsoft 365 admin center doesn't provide a way to directly print the displayed list.

Fortunately, you can use PowerShell to not only display the list but to save it to a file that can be easily imported into Excel. Here's an example command to save Skype for Business Online user data to a comma-separated values (CSV) file, which can then be easily imported as a table in an Excel worksheet:

```
Get-CsOnlineUser | Select DisplayName, UserPrincipalName, UsageLocation | Export-Csv -Path "C:\Logs\SfBUUsers.csv" -NoTypeInformation
```

Here's an example of the results:

	A	B	C
1	DisplayName	UserPrincipalName	UsageLocation
2	Alex Darrow	AlexD@litwareinc.onmicrosoft.com	US
3	Allie Bellew	AllieB@litwareinc.onmicrosoft.com	US
4	Anne Wallace	AnneW@litwareinc.onmicrosoft.com	US
5	Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	US
6	Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	US
7	Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	US
8	David Longmuir	DavidL@litwareinc.onmicrosoft.com	US
9	Denis Dehenne	DenisD@litwareinc.onmicrosoft.com	US
10	Garret Vargas	GarretV@litwareinc.onmicrosoft.com	US
11	Garth Fort	GarthF@litwareinc.onmicrosoft.com	US
12	Janet Schorr	JanetS@litwareinc.onmicrosoft.com	US

The interpretation of this PowerShell command is: Get all the Skype for Business Online users in the current Microsoft 365 subscription (**Get-CsOnlineUser**); obtain only the user name, UPN, and location (**Select DisplayName, UserPrincipalName, UsageLocation**); and then save that information in a CSV file named `C:\Logs\SfBUsers.csv` (**Export-Csv -Path "C:\Logs\SfBUsers.csv" -NoTypeInfoInformation**).

You can also use options to save this list as an XML file or an HTML page. In fact, with additional PowerShell commands, you could save it directly as an Excel file, with any custom formatting you want.

You can also send the output of a PowerShell command that displays a list directly to the default printer in Windows. Here's an example command:

```
Get-CsOnlineUser | Select DisplayName, UserPrincipalName, UsageLocation | Out-Printer
```

Here's what your printed document will look like:

DisplayName	UserPrincipalName	UsageLocation
=====	=====	=====
Alex Darrow	AlexD@litwareinc.onmicrosoft.com	US
Allie Bellew	AllieB@litwareinc.onmicrosoft.com	US
Anne Wallace	AnneW@litwareinc.onmicrosoft.com	US
Aziz Hassouneh	AzizH@litwareinc.onmicrosoft.com	US
Belinda Newman	BelindaN@litwareinc.onmicrosoft.com	US
Bonnie Kearney	BonnieK@litwareinc.onmicrosoft.com	US
David Longmuir	DavidL@litwareinc.onmicrosoft.com	US
Denis Dehenne	DenisD@litwareinc.onmicrosoft.com	US
Garret Vargas	GarretV@litwareinc.onmicrosoft.com	US
Garth Fort	GarthF@litwareinc.onmicrosoft.com	US
Janet Schorr	JanetS@litwareinc.onmicrosoft.com	US

The interpretation of this PowerShell command is: Get all the Skype for Business Online users in the current Microsoft 365 subscription; obtain only the user name, UPN, and location; and then send that information to the default Windows printer (**Out-Printer**).

The printed document has the same simple formatting as the display in the PowerShell command window. To get a hard copy, just add **| Out-Printer** to the end of the command.

PowerShell for Microsoft 365 lets you manage across server products

The components that make up Microsoft 365 are designed to work together. For example, suppose you add a

new user to Microsoft 365, and you specify such information as the user's department and phone number. That information will then be available if you access the user's information in any of the Microsoft 365 services: Skype for Business Online, Exchange, or SharePoint.

But that's for common information that spans the suite of products. Product-specific information, such as information about a user's Exchange mailbox, isn't typically available across the suite. For example, information about whether a user's mailbox is enabled or not is available only in the Exchange admin center.

Suppose you'd like to make a report that shows the following information for all your users:

- The user's display name
- Whether the user is licensed for Microsoft 365
- Whether the user's Exchange mailbox has been enabled
- Whether the user is enabled for Skype for Business Online

You can't easily produce such a report in the Microsoft 365 admin center. Instead, you would have to create a separate document to store the information, such as an Excel worksheet. Then, get all the user names and licensing information from the Microsoft 365 admin center, get mailbox information from the [Exchange admin center](#), get Skype for Business Online information from the Skype for Business Online Admin center, and then combine that information.

The alternative is to use a PowerShell script to compile the report for you.

The following example script is more complicated than the commands you've seen so far in this article. But, it shows the potential of using PowerShell to create information views that are difficult to get otherwise. Here's the script to compile and display the list you need:

```
$x = Get-AzureADUser

foreach ($i in $x)
{
    $y = Get-Mailbox -Identity $i.UserPrincipalName
    $i | Add-Member -MemberType NoteProperty -Name IsMailboxEnabled -Value $y.IsMailboxEnabled

    $y = Get-CsOnlineUser -Identity $i.UserPrincipalName
    $i | Add-Member -MemberType NoteProperty -Name EnabledForSfB -Value $y.Enabled
}

$x | Select DisplayName, IsLicensed, IsMailboxEnabled, EnabledForSfB
```

Here's an example of the results:

DisplayName	IsLicensed	IsMailboxEnabled	EnabledForSfB
Bonnie Kearney	True	True	True
Fabrice Canel	True	True	True
Brian Johnson	False	True	False
Anne Wallace	True	True	True
Alex Darrow	True	True	True
David Longmuir	True	True	True
Katy Jordan	False	True	False
Molly Dempsey	False	True	False

The interpretation of this PowerShell script is:

1. Get all the users in the current Microsoft 365 subscription and store the information in a variable that's named `$x` (`$x = Get-AzureADUser`).

2. Start a loop that runs over all the users in the variable `$x` (**foreach (\$i in \$x)**).
3. Define a variable named `$y` and store the user's mailbox information in it (**\$y = Get-Mailbox -Identity \$i.UserPrincipalName**).
4. Add a new property to the user information that's named *IsMailBoxEnabled*. Set it to the value of the `IsMailBoxEnabled` property of the user's mailbox (**\$i | Add-Member -MemberType NoteProperty -Name IsMailboxEnabled -Value \$y.IsMailboxEnabled**).
5. Define a variable named `$y`, and store the user's Skype for Business Online information in it (**\$y = Get-CsOnlineUser -Identity \$i.UserPrincipalName**).
6. Add a new property to the user information that's named *EnabledForSfB*. Set it to the value of the `Enabled` property of the user's Skype for Business Online information (**\$i | Add-Member -MemberType NoteProperty -Name EnabledForSfB -Value \$y.Enabled**).
7. Display the list of users, but include only their name, whether they are licensed, and the two new properties that indicate whether their mailbox is enabled and whether they are enabled for Skype for Business Online (**\$x | Select DisplayName, IsLicensed, IsMailboxEnabled, EnabledforSfB**).

See also

[Get started with PowerShell for Microsoft 365](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Use Windows PowerShell to create reports in Microsoft 365](#)

Connect to Microsoft 365 with PowerShell

10/28/2022 • 7 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

PowerShell for Microsoft 365 enables you to manage your Microsoft 365 settings from the command line. To connect to PowerShell, just install the required software and then connect to your Microsoft 365 organization.

There are two versions of the PowerShell module that you can use to connect to Microsoft 365 and administer user accounts, groups, and licenses:

- Azure Active Directory PowerShell for Graph, whose cmdlets include *AzureAD* in their name
- Microsoft Azure Active Directory Module for Windows PowerShell, whose cmdlets include *Mso/* in their name

Currently, the Azure Active Directory PowerShell for Graph module doesn't completely replace the functionality of the Microsoft Azure Active Directory Module for Windows PowerShell module for user, group, and license administration. In some cases, you need to use both versions. You can safely install both versions on the same computer.

NOTE

You can also connect with the [Azure Cloud Shell](#) from the Microsoft 365 admin center.

What do you need to know before you begin?

NOTE

The Azure Active Directory Module is being replaced by the Microsoft Graph PowerShell SDK. You can use the Microsoft Graph PowerShell SDK to access all Microsoft Graph APIs. For more information, see [Get started with the Microsoft Graph PowerShell SDK](#).

Operating system

You must use a 64-bit version of Windows. Support for the 32-bit version of the Microsoft Azure Active Directory Module for Windows PowerShell ended in 2014.

You can use the following versions of Windows:

- Windows 10, Windows 8.1, Windows 8, or Windows 7 Service Pack 1 (SP1)
- Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 SP1

NOTE

For Windows 8.1, Windows 8, Windows 7 Service Pack 1 (SP1), Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 SP1, download and install the [Windows Management Framework 5.1](#).

PowerShell

- For the Azure Active Directory PowerShell for Graph module, you must use PowerShell version 5.1.
- For the Microsoft Azure Active Directory Module for Windows PowerShell module, you must use PowerShell version 5.1 or later, up to PowerShell version 6. You can't use PowerShell version 7.

NOTE

These procedures are intended for users who are members of a Microsoft 365 admin role. For more information, see [About admin roles](#).

Connect with the Azure Active Directory PowerShell for Graph module

Commands in the Azure Active Directory PowerShell for Graph module have *AzureAD* in their cmdlet name. You can install the [Azure Active Directory PowerShell for Graph](#) module or [Azure PowerShell](#).

For procedures that require the new cmdlets in the Azure Active Directory PowerShell for Graph module, follow these steps to install the module and connect to your Microsoft 365 subscription.

NOTE

For information about support for different versions of Windows, see [Azure Active Directory PowerShell for Graph module](#).

Step 1: Install the required software

These steps are required only one time on your computer. But you'll likely need to update the software periodically.

1. Open a Windows PowerShell Command Prompt window.
2. Run this command:

```
Install-Module -Name AzureAD
```

By default, the PowerShell Gallery (PSGallery) isn't configured as a trusted repository for **PowerShellGet**. The first time you use the PSGallery, you'll see the following message:

Untrusted repository

You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the `Set-PSRepository` cmdlet.

Are you sure you want to install the modules from 'PSGallery'?

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):

Answer **Yes** or **Yes to All** to continue with the installation.

3. Run this command to import the module:

```
Import-Module AzureAD
```

Step 2: Connect to Azure AD for your Microsoft 365 subscription

To connect to Azure Active Directory (Azure AD) for your Microsoft 365 subscription with an account name and

password or with multi-factor authentication, run one of these commands from a Windows PowerShell command prompt. (It doesn't have to be elevated.)

OFFICE 365 CLOUD	COMMAND
Office 365 Worldwide (+GCC)	<code>Connect-AzureAD</code>
Office 365 operated by 21 Vianet	<code>Connect-AzureAD -AzureEnvironmentName AzureChinaCloud</code>
Office 365 Germany	<code>Connect-AzureAD -AzureEnvironmentName AzureGermanyCloud</code>
Office 365 U.S. Government DoD and Office 365 U.S. Government GCC High	<code>Connect-AzureAD -AzureEnvironmentName AzureUSGovernment</code>

In the **Sign into your account** dialog box, type your Microsoft 365 work or school account user name and password, and then select **OK**.

If you're using multi-factor authentication, follow the instructions to provide additional authentication information, such as a verification code.

After you connect, you can use the cmdlets for the [Azure Active Directory PowerShell for Graph module](#).

Connect with the Microsoft Azure Active Directory Module for Windows PowerShell

NOTE

Cmdlets in the Microsoft Azure Active Directory Module for Windows PowerShell have *Mso/* in their name.

PowerShell version 7 and later don't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso/* in their name. For PowerShell version 7 and later, you must use the Microsoft Graph PowerShell SDK.

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso/* in their name. Run these cmdlets from Windows PowerShell.

Step 1: Install the required software

These steps are required only one time on your computer. But you'll likely need to update the software periodically.

1. If you're not running Windows 10, install the 32-bit version of the Microsoft Online Services Sign-in Assistant: [Microsoft Online Services Sign-in Assistant for IT Professionals RTW](#).
2. Follow these steps to install the Microsoft Azure Active Directory Module for Windows PowerShell:
 - a. Open an elevated Windows PowerShell command prompt (run Windows PowerShell as an administrator).
 - b. Run the **Install-Module MSOnline** command.
 - c. If you're prompted to install the NuGet provider, type **Y** and press Enter.
 - d. If you're prompted to install the module from PSGallery, type **Y** and press Enter.

Step 2: Connect to Azure AD for your Microsoft 365 subscription

To connect to Azure AD for your Microsoft 365 subscription with an account name and password or with multi-factor authentication, run one of these commands from a Windows PowerShell command prompt. (It doesn't have to be elevated.)

OFFICE 365 CLOUD	COMMAND
Office 365 Worldwide (+GCC)	<code>Connect-MsolService</code>
Office 365 operated by 21 Vianet	<code>Connect-MsolService -AzureEnvironment AzureChinaCloud</code>
Office 365 Germany	<code>Connect-MsolService -AzureEnvironment AzureGermanyCloud</code>
Office 365 U.S. Government DoD and Office 365 U.S. Government GCC High	<code>Connect-MsolService -AzureEnvironment USGovernment</code>

In the **Sign into your account** dialog box, type your Microsoft 365 work or school account user name and password, and then select **OK**.

If you're using multi-factor authentication, follow the instructions to provide additional authentication information, such as a verification code.

How do you know it worked?

If you don't get an error message, you connected successfully. For quick test, run a Microsoft 365 cmdlet, such as **Get-MsolUser**, and see the results.

If you get an error message, check the following issues:

- **A common problem is an incorrect password.** Run [Step 2](#) again, and pay close attention to the user name and password that you enter.
- **The Microsoft Azure Active Directory Module for Windows PowerShell requires that Microsoft .NET Framework 3.5.x is enabled on your computer.** It's likely that your computer has a newer version installed (for example, 4 or 4.5.x). But backward compatibility with older versions of the .NET Framework can be enabled or disabled. For more information, see the following articles:
 - For Windows Server 2012 or Windows Server 2012 R2, see [Enable .NET Framework 3.5 by using the Add Roles and Features Wizard](#).
 - For Windows 7 or Windows Server 2008 R2, see [You can't open the Azure Active Directory Module for Windows PowerShell](#).
 - For Windows 10, Windows 8.1, and Windows 8, see [Install the .NET Framework 3.5 on Windows 10, Windows 8.1, and Windows 8](#).
- **Your version of the Microsoft Azure Active Directory Module for Windows PowerShell might be out of date.** To check, run the following command in PowerShell for Microsoft 365 or the Microsoft Azure Active Directory Module for Windows PowerShell:

```
(Get-Item
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSOnline\Microsoft.Online.Administration.Automation.PSModule.dll).VersionInfo.FileVersion
```

If the version number returned is lower than *1.0.8070.2*, uninstall the Microsoft Azure Active Directory Module for Windows PowerShell and install from [Step 1](#), above.

- If you get a connection error message, see ["Connect-MsolService: Exception of type was thrown" error](#).
- If you get a "Get-Item: Cannot find path" error message, run this command:

```
(dir "C:\Program Files\WindowsPowerShell\Modules\MSOnline").Name
```

Connect with the Azure Cloud Shell

To connect with and use the Azure Cloud Shell from the Microsoft 365 admin center, select the PowerShell window icon from the upper-right corner of the task bar. In the **Welcome to Azure Cloud Shell** pane, select **PowerShell**.

You will need an active Azure subscription for your organization that is tied to your Microsoft 365 subscription. If you don't already have one, you can create one. Once you have an Azure subscription, a PowerShell window opens from which you can run PowerShell commands and scripts.

For more information, see [Azure Cloud Shell](#).

See also

- [Manage Microsoft 365 with PowerShell](#)
- [Get started with PowerShell for Microsoft 365](#)
- [Connect to all Microsoft 365 services in a single Windows PowerShell window](#)

Connect to all Microsoft 365 services in a single PowerShell window

10/28/2022 • 5 minutes to read • [Edit Online](#)

When you use PowerShell to manage Microsoft 365, you can have multiple PowerShell sessions open at the same time. You might have different PowerShell windows to manage user accounts, SharePoint Online, Exchange Online, Microsoft Teams, Microsoft Defender for Office 365 features (security), and Microsoft Purview compliance features.

This scenario isn't optimal for managing Microsoft 365, because you can't exchange data among those windows for cross-service management. This article describes how to use a single instance of PowerShell to manage Microsoft 365 accounts, Exchange Online, SharePoint Online, Microsoft Teams, and features in Defender for Office 365 Microsoft Purview compliance.

NOTE

This article currently only contains the commands to connect to the Worldwide (+GCC) cloud. Notes provide links to articles about connecting to the other Microsoft 365 clouds.

Before you begin

Before you can manage all of Microsoft 365 from a single instance of PowerShell, consider the following prerequisites:

- The Microsoft 365 work or school account that you use must be a member of a Microsoft 365 admin role. For more information, see [About admin roles](#). This is a requirement for PowerShell for Microsoft 365, but not necessarily for all other Microsoft 365 services.
- You can use the following 64-bit versions of Windows:
 - Windows 11
 - Windows 10
 - Windows 8.1 or Windows 8
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2 or Windows Server 2012
 - Windows 7 Service Pack 1 (SP1)*
 - Windows Server 2008 R2 SP1*

* You need to install Microsoft .NET Framework 4.5.x and then Windows Management Framework 3.0 or 4.0. For more information, see [Windows Management Framework](#).

- You need to install the modules that are required for Azure Active Directory (Azure AD), Exchange Online, Defender for Office 365, Microsoft Purview compliance, SharePoint Online, and Teams:
 - [Azure Active Directory V2](#)

- [SharePoint Online Management Shell](#)
- [Teams PowerShell Module](#)
- [Install and maintain the Exchange Online PowerShell module](#)
- [Teams PowerShell Overview](#)
- PowerShell must be configured to run signed scripts for Exchange Online, Defender for Office 365, and Microsoft Purview compliance. Run the following command in an elevated PowerShell session (a PowerShell session that you **Run as administrator**).

```
Set-ExecutionPolicy RemoteSigned
```

Connection steps when using just a password

Follow these steps to connect to all the services in a single PowerShell window when you're using just a password for sign-in.

1. Open Windows PowerShell.
2. Run this command and enter your Microsoft 365 work or school account credentials.

```
$credential = Get-Credential
```

3. Run this command to connect to Azure AD by using the Azure Active Directory PowerShell for Graph module.

```
Connect-AzureAD -Credential $credential
```

Or if you're using the Microsoft Azure Active Directory Module for Windows PowerShell module, run this command.

```
Connect-MsolService -Credential $credential
```

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso* in their name. You must run these cmdlets from PowerShell.

4. Run these commands to connect to SharePoint Online. Specify the organization name for your domain. For example, for "litwareinc.onmicrosoft.com", the organization name value is "litwareinc".

```
$orgName="<for example, litwareinc for litwareinc.onmicrosoft.com>"  
Import-Module Microsoft.Online.SharePoint.PowerShell -DisableNameChecking  
Connect-SPOService -Url https://$orgName-admin.sharepoint.com -Credential $Credential
```

5. Run these commands to connect to Exchange Online.

```
Import-Module ExchangeOnlineManagement  
Connect-ExchangeOnline -ShowProgress $true
```

NOTE

To connect to Exchange Online for Microsoft 365 clouds other than Worldwide, see [Connect to Exchange Online PowerShell](#).

6. Run these commands to connect to Security & Compliance PowerShell.

```
$acctName="<UPN of the account, such as belindan@litwareinc.onmicrosoft.com>"  
Connect-IPPSession -UserPrincipalName $acctName
```

NOTE

To connect to Security & Compliance PowerShell for Microsoft 365 clouds other than Worldwide, see [Connect to Security & Compliance PowerShell](#).

7. Run these commands to connect to Teams PowerShell.

```
Import-Module MicrosoftTeams  
$credential = Get-Credential  
Connect-MicrosoftTeams -Credential $credential
```

NOTE

Skype for Business Online Connector is currently part of the latest Teams PowerShell module. If you're using the latest Teams PowerShell public release, you don't need to install the Skype for Business Online Connector.

To connect to Microsoft Teams clouds other than *Worldwide*, see [Connect-MicrosoftTeams](#).

Azure Active Directory PowerShell for Graph module when using just a password

Here are the commands for all the services in a single block when you use the Azure Active Directory PowerShell for Graph module. Specify the name of your domain host and the UPN for the sign-in and run them all at the same time.

```
$orgName="<for example, litwareinc for litwareinc.onmicrosoft.com>"  
$acctName="<UPN of the account, such as belindan@litwareinc.onmicrosoft.com>"  
$credential = Get-Credential -UserName $acctName -Message "Type the account's password."  
#Azure Active Directory  
Connect-AzureAD -Credential $credential  
#SharePoint Online  
Import-Module Microsoft.Online.SharePoint.PowerShell -DisableNameChecking  
Connect-SPOService -Url https://$orgName-admin.sharepoint.com -credential $credential  
#Exchange Online  
Import-Module ExchangeOnlineManagement  
Connect-ExchangeOnline -ShowProgress $true  
#Security & Compliance  
Connect-IPPSession -UserPrincipalName $acctName  
#Teams and Skype for Business Online  
Import-Module MicrosoftTeams  
Connect-MicrosoftTeams -Credential $credential
```

Microsoft Azure Active Directory Module for Windows PowerShell module when using just a password

Here are the commands for all the services in a single block when you use the Microsoft Azure Active Directory Module for Windows PowerShell module. Specify the name of your domain host and the UPN for the sign-in and run them all at one time.


```

$orgName="<for example, litwareinc for litwareinc.onmicrosoft.com>"
$acctName="<UPN of the account, such as belindan@litwareinc.onmicrosoft.com>"
$credential = Get-Credential -UserName $acctName -Message "Type the account's password."
#Azure Active Directory
Connect-MsolService -Credential $credential
#SharePoint Online
Import-Module Microsoft.Online.SharePoint.PowerShell -DisableNameChecking
Connect-SPOService -Url https://$orgName-admin.sharepoint.com -credential $credential
#Exchange Online
Connect-ExchangeOnline -ShowProgress $true
#Security & Compliance
Connect-IPPSession -UserPrincipalName $acctName
#Teams and Skype for Business Online
Import-Module MicrosoftTeams
Connect-MicrosoftTeams -Credential $credential

```

Connection steps when using multi-factor authentication

Azure Active Directory PowerShell for Graph module when using MFA

Here are all the commands in a single block to connect to multiple Microsoft 365 services when you use multi-factor authentication with the Azure Active Directory PowerShell for Graph module.

```

$acctName="<UPN of the account, such as belindan@litwareinc.onmicrosoft.com>"
$orgName="<for example, litwareinc for litwareinc.onmicrosoft.com>"
#Azure Active Directory
Connect-AzureAD
#SharePoint Online
Connect-SPOService -Url https://$orgName-admin.sharepoint.com
#Exchange Online
Connect-ExchangeOnline -UserPrincipalName $acctName -ShowProgress $true
#Security & Compliance
Connect-IPPSession -UserPrincipalName $acctName
#Teams and Skype for Business Online
Import-Module MicrosoftTeams
Connect-MicrosoftTeams

```

Microsoft Azure Active Directory Module for Windows PowerShell module when using MFA

Here are all the commands in a single block to connect to multiple Microsoft 365 services when you use multi-factor authentication with the Microsoft Azure Active Directory Module for Windows PowerShell module.

```

$acctName="<UPN of the account, such as belindan@litwareinc.onmicrosoft.com>"
$orgName="<for example, litwareinc for litwareinc.onmicrosoft.com>"
#Azure Active Directory
Connect-MsolService
#SharePoint Online
Connect-SPOService -Url https://$orgName-admin.sharepoint.com
#Exchange Online
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -UserPrincipalName $acctName -ShowProgress $true
#Security & Compliance Center
Connect-IPPSession -UserPrincipalName $acctName
#Teams and Skype for Business Online
Import-Module MicrosoftTeams
Connect-MicrosoftTeams

```

Close the PowerShell window

To close down the PowerShell window, run this command to remove the active sessions to SharePoint Online,

Teams, Defender for Office 365 and Microsoft Purview compliance:

```
Disconnect-SPOService; Disconnect-MicrosoftTeams; Disconnect-ExchangeOnline
```

See also

- [Connect to Microsoft 365 with PowerShell](#)
- [Manage SharePoint Online with PowerShell](#)
- [Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

Use PowerShell to create reports for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Many different reports are available in the Microsoft 365 admin center. But these reports only provide so much information, and sometimes you need more. That's when you need PowerShell for Microsoft 365.

These articles describe how to use PowerShell for Microsoft 365 to get information from your Microsoft 365 tenant:

- Get started with reporting using PowerShell for Microsoft 365:
 - [Why you need to use PowerShell for Microsoft 365](#)
- Reports for user accounts and licenses:
 - [View Microsoft 365 licenses and services with PowerShell](#)
 - [View Microsoft 365 licensed and unlicensed users with PowerShell](#)
 - [View Microsoft 365 account license and service details with PowerShell](#)
 - [View Microsoft 365 user accounts with PowerShell](#)
- Reports for SharePoint Online:
 - [Get started with SharePoint Online Management Shell](#)
 - [Get-SPOSiteGroup - Gets all the groups on a specified site collection](#)
- Reports for Exchange Online:
 - [Use Exchange Online PowerShell to display mailbox](#)

Related articles

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

[Manage SharePoint with PowerShell](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

Cmdlet references for Microsoft 365 services

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

This article provides cmdlet references for the various Microsoft 365 services and connection instructions for each Microsoft 365 service that PowerShell supports.

NOTE

To connect to all services at once, see [Connect to all Microsoft 365 services in a single Windows PowerShell window](#).

Azure Active Directory PowerShell cmdlets

The Azure Active Directory PowerShell for Graph cmdlet reference topics are in the Reference section of the [Azure Active Directory PowerShell for Graph documentation](#).

The Azure Active Directory Module for Windows PowerShell cmdlet reference topics is in the Reference section of the [Azure Active Directory \(MSOnline\) documentation](#).

For Microsoft 365 PowerShell connection instructions, see [Connect to Microsoft 365 with PowerShell](#).

Exchange Online PowerShell cmdlets

Exchange Online cmdlet reference topics are in the Reference section of the [Exchange Online PowerShell documentation](#).

For connection instructions for Exchange Online PowerShell, see [Connect to Exchange Online PowerShell](#).

NOTE

Reporting cmdlets for other services, such as SharePoint Online, Skype for Business Online, and Microsoft 365 user activity, are available in Exchange Online PowerShell. For more information, see [Reporting cmdlets in Exchange Online](#).

SharePoint Online PowerShell cmdlets

For SharePoint Online cmdlets, see [Index of Windows PowerShell for SharePoint Online cmdlets](#).

For connection instructions for SharePoint Online PowerShell, see [Set up the SharePoint Online Management Shell Windows PowerShell environment](#).

Skype for Business Online PowerShell cmdlets

For Skype for Business Online cmdlet reference topics, see [Skype for Business Online cmdlets](#).

For connection instructions for Skype for Business Online PowerShell, see [Manage Skype for Business Online with PowerShell](#).

Security & Compliance PowerShell cmdlets

The Security & Compliance Center cmdlet references are in the Reference section of the [Security & Compliance](#)

[PowerShell documentation.](#)

For connection instructions for Security & Compliance PowerShell, see [Connect to the Security & Compliance PowerShell](#).

See also

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Microsoft 365 community resources for PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

Connect to these communities to reach your peers and get answers for your PowerShell for Microsoft 365 questions.

- [Microsoft 365 Microsoft Tech Community](#)
- [Exchange Server TechNet community forum](#)

See also

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Manage Microsoft 365 user accounts, licenses, and groups with PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 administrators need to manage user accounts, licenses, and groups. Although you can do most of these tasks in the Microsoft 365 admin center, some are easier in PowerShell.

For more information, see the following articles.

User accounts

- [Create user accounts](#)
- [View user accounts](#)
- [Configure user account properties](#)
- [Assign roles to user accounts](#)
- [Delete and restore user accounts](#)
- [Block user accounts](#)
- [Passwords](#)

Licenses and services

- [View licenses and services](#)
- [View licensed and unlicensed users](#)
- [Assign licenses to user accounts](#)
- [View account license and service details](#)
- [Disable access to services](#)
 - [Disable access to Sway](#)
 - [Disable access to services while assigning user licenses](#)
- [Remove licenses from user accounts](#)

Groups

- [Manage security groups](#)
- [Maintain security group membership](#)
- [Manage Microsoft 365 groups](#)

Create Microsoft 365 user accounts with PowerShell

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use PowerShell for Microsoft 365 to efficiently create user accounts, including multiple accounts.

When you create user accounts in PowerShell, certain account properties are always required. Other properties aren't required but are important. See the following table.

PROPERTY NAME	REQUIRED?	DESCRIPTION
DisplayName	Yes	This is the display name that's used in Microsoft 365 services. For example, <i>Caleb Sills</i> .
UserPrincipalName	Yes	This is the account name that's used to sign in to Microsoft 365 services. For example, <i>CalebS@contoso.onmicrosoft.com</i> .
FirstName	No	
LastName	No	
LicenseAssignment	No	This is the licensing plan (also known as the license plan or SKU) from which an available license is assigned to the user account. The license defines the Microsoft 365 services that are available to the account. You don't have to assign a license to a user when you create the account, but the account must have a license to access Microsoft 365 services. You have 30 days to license the user account after you create it.
Password	No	If you don't specify a password, a random password is assigned to the user account, and the password is visible in the results of the command. If you specify a password, it needs to be 8 to 16 ASCII text characters of the following types: lowercase letters, uppercase letters, numbers, and symbols.

PROPERTY NAME	REQUIRED?	DESCRIPTION
UsageLocation	No	This is a valid ISO 3166-1 alpha-2 country code. For example, <i>US</i> for the United States, and <i>FR</i> for France. It's important to provide this value, because some Microsoft 365 services aren't available in certain countries. You can't assign a license to a user account unless the account has this value configured. For more information, see About license restrictions .

NOTE

Learn how to create user accounts by using the Microsoft 365 admin center.

For a list of additional resources, see [Manage users and groups](#).

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

After you connect, use the following syntax to create an individual account:

```
$PasswordProfile=New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
$PasswordProfile.Password="<user account password>"
New-AzureADUser -DisplayName "<display name>" -GivenName "<first name>" -SurName "<last name>" -
UserPrincipalName <sign-in name> -UsageLocation <ISO 3166-1 alpha-2 country code> -MailNickName <mailbox
name> -PasswordProfile $PasswordProfile -AccountEnabled $true
```

This example creates an account for the US user *Caleb Sills*:

```
$PasswordProfile=New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
$PasswordProfile.Password="3Rv0y1q39/chsy"
New-AzureADUser -DisplayName "Caleb Sills" -GivenName "Caleb" -SurName "Sills" -UserPrincipalName
calebs@contoso.onmicrosoft.com -UsageLocation US -MailNickName calebs -PasswordProfile $PasswordProfile -
AccountEnabled $true
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

Create an individual user account

To create an individual account, use the following syntax:

```
New-MsolUser -DisplayName <display name> -FirstName <first name> -LastName <last name> -UserPrincipalName
<sign-in name> -UsageLocation <ISO 3166-1 alpha-2 country code> -LicenseAssignment <licensing plan name> [-
Password <Password>]
```

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets that have *Mso* in their name. Run these cmdlets from Windows PowerShell.

To list the available [licensing plan names](#), use this command:

```
Get-MsolAccountSku
```

This example creates an account for the US user *Caleb Sills*, and assigns a license from the `contoso:ENTERPRISEPACK` (Office 365 Enterprise E3) licensing plan.

```
New-MsolUser -DisplayName "Caleb Sills" -FirstName Caleb -LastName Sills -UserPrincipalName  
calebs@contoso.onmicrosoft.com -UsageLocation US -LicenseAssignment contoso:ENTERPRISEPACK
```

Create multiple user accounts

1. Create a comma-separated value (CSV) file that contains the required user account information. For example:

```
UserPrincipalName,FirstName,LastName,DisplayName,UsageLocation,AccountSkuId  
ClaudeL@contoso.onmicrosoft.com,Claude,Loiselle,Claude Loiselle,US,contoso:ENTERPRISEPACK  
LynneB@contoso.onmicrosoft.com,Lynne,Baxter,Lynne Baxter,US,contoso:ENTERPRISEPACK  
ShawnM@contoso.onmicrosoft.com,Shawn,Melendez,Shawn Melendez,US,contoso:ENTERPRISEPACK
```

NOTE

The column names and their order in the first row of the CSV file are arbitrary. But make sure the order of the data in the rest of the file matches the order of the column names. And use the column names for the parameter values in the PowerShell for Microsoft 365 command.

2. Use the following syntax:

```
Import-Csv -Path <Input CSV File Path and Name> | foreach {New-MsolUser -DisplayName $_.DisplayName  
-FirstName $_.FirstName -LastName $_.LastName -UserPrincipalName $_.UserPrincipalName -UsageLocation  
$_.UsageLocation -LicenseAssignment $_.AccountSkuId [-Password $_.Password]} | Export-Csv -Path  
<Output CSV File Path and Name>
```

This example creates user accounts from the file *C:\My Documents\NewAccounts.csv* and logs the results in a file named *C:\My Documents\NewAccountResults.csv*.

```
Import-Csv -Path "C:\My Documents\NewAccounts.csv" | foreach {New-MsolUser -DisplayName  
$_.DisplayName -FirstName $_.FirstName -LastName $_.LastName -UserPrincipalName $_.UserPrincipalName  
-UsageLocation $_.UsageLocation -LicenseAssignment $_.AccountSkuId} | Export-Csv -Path "C:\My  
Documents\NewAccountResults.csv"
```

3. Review the output file to see the results. We didn't specify passwords, so the random passwords that Microsoft 365 generated are visible in the output file.

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

View Microsoft 365 user accounts with PowerShell

10/28/2022 • 8 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use the Microsoft 365 admin center to view the accounts for your Microsoft 365 tenant. PowerShell for Microsoft 365 enables this but also provides additional functionality.

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

View all accounts

To display the full list of user accounts, run this command:

```
Get-AzureADUser
```

You should get information similar to this:

ObjectId	DisplayName	UserPrincipalName
-----	-----	-----
032fc1fc-b5a2-46f1-8635-3d7dc52c48d	Adele Vance	
AdeleV@litwareinc.OnMicr...		
bd1e6af1-41e7-4f77-a2ac-5b209950135c	Global Administrator	
admin@litwareinc.onmicro...		
ec37a4d6-232e-4eb7-82a5-1613490642a5	Alex Wilber	
AlexW@litwareinc.OnMicro...		
be4bddd-c790-424c-9f96-a0cf609b7815	Allan Deyoung	
AllanD@litwareinc.OnMicr...		
598ab87b-76f0-4bf9-9538-bd46b10f4438	Christie Cline	
ChristieC@litwareinc.OnM...		
40722671-e520-4a5f-97d4-0bc9e9b2dc0f	Debra Berger	
DebraB@litwareinc.OnMicr...		

View a specific account

To display a specific user account, run the following command. Fill in the sign-in account name of the user account, which is also known as the user principal name (UPN). Remove the "<" and ">" characters.

```
Get-AzureADUser -ObjectId <sign-in name of the user account>
```

Here's an example:

```
Get-AzureADUser -ObjectId BelindaN@litwareinc.onmicrosoft.com
```

View additional property values for a specific account

By default, the `Get-AzureADUser` cmdlet only displays the *ObjectId*, *DisplayName*, and *UserPrincipalName* properties of accounts.

To be more selective about the properties to display, use the `Select` cmdlet in combination with the `Get-AzureADUser` cmdlet. To combine the two cmdlets, use the "pipe" character ("`|`"), which tells Azure Active Directory PowerShell for Graph to take the results of one command and send it to the next command. Here's an

example command that displays the *DisplayName*, *Department*, and *UsageLocation* for every user account:

```
Get-AzureADUser | Select DisplayName,Department,UsageLocation
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-AzureADUser**) and send it to the next command (**|**).
2. Display only the user account name, department, and usage location (**Select DisplayName, Department, UsageLocation**).

To see all the properties for a specific user account, use the **Select** cmdlet and the wildcard character (*). Here's an example:

```
Get-AzureADUser -ObjectID BelindaN@litwareinc.onmicrosoft.com | Select *
```

As another example, run the following command to check the enabled status of a specific user account:

```
Get-AzureADUser -ObjectID <sign-in name of the user account> | Select  
DisplayName,UserPrincipalName,AccountEnabled
```

View account synchronization status

User accounts have two sources:

- Windows Server Active Directory (AD), which are accounts that sync from on-premises AD to the cloud.
- Azure Active Directory (Azure AD) accounts, which are created directly in the cloud.

You can use the following command to find accounts that are synchronizing from **on-premise** AD. It instructs PowerShell to get all users who have the attribute *DirSyncEnabled* set to *True*.

```
Get-AzureADUser | Where {$_.DirSyncEnabled -eq $true}
```

You can use the following command to find **cloud-only** accounts. It instructs PowerShell to get all users who have the attribute *DirSyncEnabled* set to *False* or not set (*Null*). An account that was never synced from on-premise AD has *DirSyncEnabled* set to *Null*. An account that was synced initially from on-premise AD but is no longer being synced has *DirSyncEnabled* set to *False*.

```
Get-AzureADUser | Where {$_.DirSyncEnabled -ne $true}
```

View accounts based on a common property

To be more selective about the list of accounts to display, you can use the **Where** cmdlet in combination with the **Get-AzureADUser** cmdlet. To combine the two cmdlets, use the "pipe" character ("**|**"), which tells Azure Active Directory PowerShell for Graph to take the results of one command and send it to the next command. Here's an example command that displays only those user accounts that have an unspecified usage location:

```
Get-AzureADUser | Where {$_.UsageLocation -eq $Null}
```

This command instructs Azure Active Directory PowerShell for Graph to:

1. Get all the information on the user accounts (**Get-AzureADUser**) and send it to the next command (**|**).
2. Find all the user accounts that have an unspecified usage location (**Where {\$_.UsageLocation -eq**

\$Null}). Inside the braces, the command instructs PowerShell to only find the set of accounts for which the UsageLocation user account property (**\$_UsageLocation**) is not specified (**-eq \$Null**).

The **UsageLocation** property is only one of many properties associated with a user account. To display all the properties for a specific user account, use the **Select** cmdlet and the wildcard character (*). Here's an example:

```
Get-AzureADUser -ObjectID BelindaN@litwareinc.onmicrosoft.com | Select *
```

For example, **City** is the name of a user account property. You can use the following command to list all accounts of users who live in London:

```
Get-AzureADUser | Where {$_.City -eq "London"}
```

TIP

The syntax for the **Where** cmdlet in these examples is **Where {\$_. [user account property name] [comparison operator] [value] }.** > [comparison operator] is **-eq** for equals, **-ne** for not equals, **-lt** for less than, **-gt** for greater than, and others. [value] is typically a string (a sequence of letters, numbers, and other characters), a numerical value, or **\$Null** for unspecified. For more information, see [Where](#).

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

View all accounts

To display the full list of user accounts, run this command:

```
Get-MsolUser
```

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso* in their name. Run these cmdlets from Windows PowerShell.

You should get information similar to this:

UserPrincipalName	DisplayName	islicensed
-----	-----	-----
BonnieK@litwareinc.onmicrosoft.com	Bonnie Kearney	True
FabriceC@litwareinc.onmicrosoft.com	Fabrice Canel	True
BrianJ@litwareinc.onmicrosoft.com	Brian Johnson	False
AnneW@litwareinc.onmicrosoft.com	Anne Wallace	True
ScottW@litwareinc.onmicrosoft.com	Scott Wallace	False

The **Get-MsolUser** cmdlet also has a set of parameters to filter the set of user accounts displayed. For example, for the list of unlicensed users (users who have been added to Microsoft 365 but haven't yet been licensed to use any of the services), run this command:

```
Get-MsolUser -UnlicensedUsersOnly
```

You should get information similar to this:

UserPrincipalName	DisplayName	islicensed
-----	-----	-----
BrianJ@litwareinc.onmicrosoft.com	Brian Johnson	False
ScottW@litwareinc.onmicrosoft.com	Scott Wallace	False

For information about additional parameters to filter the set of user accounts that are displayed, see [Get-MsolUser](#).

View a specific account

To display a specific user account, run the following command. Fill in the sign-in name of the user account, which is also known as the user principal name (UPN). Remove the "<" and ">" characters.

```
Get-MsolUser -UserPrincipalName <sign-in name of the user account>
```

View accounts based on a common property

To be more selective about the list of accounts to display, you can use the **Where** cmdlet in combination with the **Get-MsolUser** cmdlet. To combine the two cmdlets, use the "pipe" character ("|"), which tells PowerShell to take the results of one command and send it to the next command. Here's an example that displays only those user accounts that have an unspecified usage location:

```
Get-MsolUser | Where {$_.UsageLocation -eq $Null}
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-MsolUser**) and send it to the next command (|).
2. Find all user accounts that have an unspecified usage location (**Where {\$_.UsageLocation -eq \$Null}**). Inside the braces, the command instructs PowerShell to find only the set of accounts for which the UsageLocation user account property (**\$_UsageLocation**) is not specified (**-eq \$Null**).

You should get information similar to this:

UserPrincipalName	DisplayName	islicensed
-----	-----	-----
BrianJ@litwareinc.onmicrosoft.com	Brian Johnson	False
ScottW@litwareinc.onmicrosoft.com	Scott Wallace	False

The *UsageLocation* property is only one of many properties associated with a user account. To see all of the properties for user accounts, use the **Select** cmdlet and the wildcard character (*) to display them all for a specific user account. Here's an example:

```
Get-MsolUser -UserPrincipalName BelindaN@litwareinc.onmicrosoft.com | Select *
```

For example, *City* is the name of a user account property. You can use the following command to list all of the user accounts for users who live in London:

```
Get-MsolUser | Where {$_.City -eq "London"}
```

TIP

The syntax for the **Where** cmdlet in these examples is **Where** {\$_ [user account property name] [comparison operator] [value] }. [comparison operator] is **-eq** for equals, **-ne** for not equals, **-lt** for less than, **-gt** for greater than, and others. [value] is typically a string (a sequence of letters, numbers, and other characters), a numerical value, or **\$Null** for unspecified. For more information, see [Where](#).

To check the blocked status of a user account, use the following command:

```
Get-MsolUser -UserPrincipalName <UPN of user account> | Select DisplayName,BlockCredential
```

View additional property values for accounts

By default, the **Get-MsolUser** cmdlet displays these three properties of user accounts:

- UserPrincipalName
- DisplayName
- isLicensed

If you need additional properties, such as the department where the user works and the country/region where they use Microsoft 365 services, you can run **Get-MsolUser** in combination with the **Select** cmdlet to specify the list of user account properties. Here's an example:

```
Get-MsolUser | Select DisplayName, Department, UsageLocation
```

This command instructs PowerShell to:

1. Get all the information about the user accounts (**Get-MsolUser**) and send it to the next command (**|**).
2. Display only the user account name, department, and usage location (**Select DisplayName, Department, UsageLocation**).

You should get information similar to this:

DisplayName	Department	UsageLocation
-----	-----	-----
Bonnie Kearney	Sales & Marketing	US
Fabrice Canel	Legal	US
Brian Johnson		
Anne Wallace	Executive Management	US
Alex Darrow	Sales & Marketing	US
Scott Wallace	Operations	

The **Select** cmdlet lets you choose what properties to display. To display all the properties for a specific user account, use the wildcard character (*). Here's an example:

```
Get-MsolUser -UserPrincipalName BelindaN@litwareinc.onmicrosoft.com | Select *
```

To be more selective about the list of accounts to display, you can also use the **Where** cmdlet. Here's an example command that displays only those user accounts that have an unspecified usage location:

```
Get-MsolUser | Where {$_ .UsageLocation -eq $Null} | Select DisplayName, Department, UsageLocation
```


This command instructs PowerShell to:

1. Get all the information about the user accounts (**Get-MsolUser**) and send it to the next command (**|**).
2. Find all user accounts that have an unspecified usage location (**Where {\$_.UsageLocation -eq \$Null}**), and send the resulting information to the next command (**|**). Inside the braces, the command instructs PowerShell to only find the set of accounts for which the UsageLocation user account property (**\$_UsageLocation**) is not specified (**-eq \$Null**).
3. Display only the user account name, department, and usage location (**Select DisplayName, Department, UsageLocation**).

You should get information similar to this:

DisplayName	Department	UsageLocation
-----	-----	-----
Brian Johnson		
Scott Wallace	Operations	

If you're using directory synchronization to create and manage your Microsoft 365 users, you can display the local account from which a Microsoft 365 user has been projected. The following example assumes that:

- Azure AD Connect is configured to use the default source anchor of ObjectGUID. (For more information about configuring a source anchor, see [Azure AD Connect: Design concepts](#)).
- The Active Directory Domain Services module for PowerShell has been installed (see [RSAT tools](#)).

```
Get-ADUser ([guid][System.Convert]::FromBase64String((Get-MsolUser -UserPrincipalName <UPN of user account>).ImmutableID)).guid
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Configure Microsoft 365 user account properties with PowerShell

10/28/2022 • 6 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use the [Microsoft 365 admin center](#) to configure properties for the user accounts of your Microsoft 365 tenant. In PowerShell, you can also do this, plus some other things you can't do in the admin center.

Use the Azure Active Directory PowerShell for Graph module

To configure properties for user accounts in the Azure Active Directory PowerShell for Graph module, use the [Set-AzureADUser](#) cmdlet and specify the properties to set or change.

First, [connect to your Microsoft 365 tenant](#).

Change properties for a specific user account

You identify the account with the *-ObjectID* parameter and set or change specific properties by using additional parameters. Here's a list of the most common parameters:

- -Department "<department name>"
- -DisplayName "<full user name>"
- -FacsimileTelephoneNumber "<fax number>"
- -GivenName "<user first name>"
- -Surname "<user last name>"
- -Mobile "<mobile phone number>"
- -JobTitle "<job title>"
- -PreferredLanguage "<language>"
- -StreetAddress "<street address>"
- -City "<city name>"
- -State "<state name>"
- -PostalCode "<postal code>"
- -Country "<country name>"
- -TelephoneNumber "<office phone number>"
- -UsageLocation "<2-character country or region code>"

This is the ISO 3166-1 alpha-2 (A2) two-letter country or region code.

For additional parameters, see [Set-AzureADUser](#).

NOTE

Before you can assign licenses to a user account, you must assign a usage location.

To display the User Principal Name for your user accounts, run the following command.

```
Get-AzureADUser | Sort UserPrincipalName | Select UserPrincipalName | More
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-AzureADUser**) and send it to the next command (**|**).
2. Sort the list of User Principal Names alphabetically (**Sort UserPrincipalName**) and send it to the next command (**|**).
3. Display just the User Principal Name property for each account (**Select UserPrincipalName**).
4. Display them one screen at a time (**More**).

To display the User Principal Name for an account based on its display name (first and last name), run the following commands. Fill in the *\$userName* variable, and remove the < and > characters:

```
$userName="<Display name>"  
Write-Host (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

This example displays the User Principal Name for the user account that has the display name *Caleb Sills*.

```
$userName="Caleb Sills"  
Write-Host (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

By using a *\$upn* variable, you can make changes to individual accounts based on their display name. Here's an example that sets *Belinda Newman's* usage location to France. But it specifies her display name rather than her User Principal Name:

```
$userName="Belinda Newman"  
$upn=(Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName  
Set-AzureADUser -ObjectID $upn -UsageLocation FR
```

Change properties for all user accounts

To change properties for all users, you can use a combination of the **Get-AzureADUser** and **Set-AzureADUser** cmdlets. The following example changes the usage location for all users to *France*.

```
Get-AzureADUser -All $true | Set-AzureADUser -UsageLocation FR
```

This command instructs PowerShell to:

1. Get all of the information on the user accounts (**Get-AzureADUser**) and send it to the next command (**|**).
2. Set the user location to France (**Set-AzureADUser -UsageLocation FR**).

Change properties for a specific set of user accounts

To change properties for a specific set of user accounts, you can use a combination of the **Get-AzureADUser**, **Where**, and **Set-AzureADUser** cmdlets. The following example changes the usage location for all the users in

the Accounting department to *France*.

```
Get-AzureADUser | Where {$_.Department -eq "Accounting"} | Set-AzureADUser -UsageLocation FR
```

This command instructs PowerShell to:

1. Get all the information on the user accounts (**Get-AzureADUser**), and send it to the next command (**|**).
2. Find all the user accounts that have their *Department* property set to "Accounting" (**Where {\$_.Department -eq "Accounting"}**), and send the resulting information to the next command (**|**).
3. Set the user location to France (**Set-AzureADUser -UsageLocation FR**).

Use the Microsoft Azure Active Directory Module for Windows PowerShell

To configure properties for user accounts with the Microsoft Azure Active Directory Module for Windows PowerShell, use the **Set-MsolUser** cmdlet and specify the properties to set or change.

First, [connect to your Microsoft 365 tenant](#).

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso* in their name. Run these cmdlets from Windows PowerShell.

Change properties for a specific user account

To configure properties for a specific user account, use the **Set-MsolUser** cmdlet and specify the properties to set or change.

You identify the account with the *-UserPrincipalName* parameter and set or change specific properties by using additional parameters. Here's a list of the most common parameters.

- -City "<city name>"
- -Country "<country name>"
- -Department "<department name>"
- -DisplayName "<full user name>"
- -Fax "<fax number>"
- -FirstName "<user first name>"
- -LastName "<user last name>"
- -MobilePhone "<mobile phone number>"
- -Office "<office location>"
- -PhoneNumber "<office phone number>"
- -PostalCode "<postal code>"
- -PreferredLanguage "<language>"
- -State "<state name>"
- -StreetAddress "<street address>"

- -Title "<title name>"
- -UsageLocation "<2-character country or region code>"

This is the ISO 3166-1 alpha-2 (A2) two-letter country or region code.

For additional parameters, see [Set-MsolUser](#).

To see the User Principal Names of all your users, run the following command:

```
Get-MsolUser | Sort UserPrincipalName | Select UserPrincipalName | More
```

This command instructs PowerShell to:

1. Get all of information for the user accounts (**Get-MsolUser**) and send it to the next command (**|**).
2. Sort the list of User Principal Names alphabetically (**Sort UserPrincipalName**) and send it to the next command (**|**).
3. Display just the User Principal Name property for each account (**Select UserPrincipalName**).
4. Display them one screen at a time (**More**).

To display the User Principal Name for an account based on its display name (first and last name), run the following commands. Fill in the *\$userName* variable, and remove the < and > characters.

```
$userName="<Display name>"
Write-Host (Get-MsolUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

This example displays the User Principal Name for the user named Caleb Sills:

```
$userName="Caleb Sills"
Write-Host (Get-MsolUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

By using a *\$upn* variable, you can make changes to individual accounts based on their display name. Here's an example that sets *Belinda Newman's* usage location to *France*, but specifies her display name rather than her User Principal Name:

```
$userName="<display name>"
$upn=(Get-MsolUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
Set-MsolUser -UserPrincipalName $upn -UsageLocation FR
```

Change properties for all user accounts

To change properties for all users, use a combination of the **Get-MsolUser** and **Set-MsolUser** cmdlets. The following example changes the usage location for all users to *France*.

```
Get-MsolUser | Set-MsolUser -UsageLocation FR
```

This command instructs PowerShell to:

1. Get all the information for the user accounts (**Get-MsolUser**) and send it to the next command (**|**).
2. Set the user location to France (**Set-MsolUser -UsageLocation FR**).

Change properties for a specific set of user accounts

To change properties for a specific set of user accounts, you can use a combination of the **Get-MsolUser**,

Where, and **Set-MsolUser** cmdlets. The following example changes the usage location for all the users in the Accounting department to *France*.

```
Get-MsolUser | Where {$_.Department -eq "Accounting"} | Set-MsolUser -UsageLocation FR
```

This command instructs PowerShell to:

1. Get all the information for the user accounts (**Get-MsolUser**) and send it to the next command (|).
2. Find all user accounts that have their *Department* property set to "Accounting" (**Where {\$_.Department -eq "Accounting"}**) and send the resulting information to the next command (|).
3. Set the user location to France (**Set-MsolUser -UsageLocation FR**).

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Assign admin roles to Microsoft 365 user accounts with PowerShell

10/28/2022 • 6 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can easily assign roles to user accounts by using PowerShell for Microsoft 365.

NOTE

Learn how to [assign admin roles](#) to user accounts with the Microsoft 365 admin center.

For a list of additional resources, see [Manage users and groups](#).

Use the Azure Active Directory PowerShell for Graph module

First, use a **Azure AD DC admin**, **Cloud Application Admin**, or **Global admin** account to [connect to your Microsoft 365 tenant](#).

For more information, see [About admin roles](#).

Next, identify the sign-in name of the user account that you want to add to a role (example: fredsm@contoso.com). This is also known as the user principal name (UPN).

Next, determine the name of the role. See [Azure AD built-in roles](#).

NOTE

Pay attention to the notes in this article. Some role names are different for Azure Active Directory (Azure AD) PowerShell. For example, the *SharePoint Administrator* role in the Microsoft 365 admin center is *SharePoint Service Administrator* in Azure AD PowerShell.

Next, fill in the sign-in and role names and run these commands:

```
$userName="<sign-in name of the account>"
$roleName="<admin role name>"
$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}
if ($role -eq $null) {
    $roleTemplate = Get-AzureADDirectoryRoleTemplate | Where {$_.displayName -eq $roleName}
    Enable-AzureADDirectoryRole -RoleTemplateId $roleTemplate.ObjectId
    $role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}
}
Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId (Get-AzureADUser | Where
{$_.UserPrincipalName -eq $userName}).ObjectID
```

Here's an example of a completed command set that assigns the SharePoint Service Administrator role to the *belindan@contoso.com* account:

```
$userName="belindan@contoso.com"
$roleName="SharePoint Service Administrator"
$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}
if ($role -eq $null) {
$roleTemplate = Get-AzureADDirectoryRoleTemplate | Where {$_.displayName -eq $roleName}
Enable-AzureADDirectoryRole -RoleTemplateId $roleTemplate.ObjectId
$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}
}
Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId (Get-AzureADUser | Where
{$_.UserPrincipalName -eq $userName}).ObjectID
```

To display the list of user names for a specific admin role, use these commands.

```
$roleName="<role name>"
Get-AzureADDirectoryRole | Where { $_.DisplayName -eq $roleName } | Get-AzureADDirectoryRoleMember | Ft
DisplayName
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, use a global administrator account to [connect to your Microsoft 365 tenant](#).

For a single role change

The most common ways to specify the user account is by using its display name or its email name, which also known as its sign-in name or user principal name (UPN).

Display names of user accounts

If you're used to working with the display names of user accounts, determine the following information:

- The user account that you want to configure

To specify the user account, you must determine its Display Name. To get a complete list of accounts, use this command:

```
Get-MsolUser -All | Sort DisplayName | Select DisplayName | More
```

This command lists the Display Name of your user accounts, sorted by the Display Name, one screen at a time. You can filter the list to a smaller set by using the **Where** cmdlet. See the following example.

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso* in their name. Run these cmdlets from Windows PowerShell.

```
Get-MsolUser -All | Where DisplayName -like "John*" | Sort DisplayName | Select DisplayName | More
```

This command lists only the user accounts for which the Display Name starts with "John".

- The role you want to assign

To display the list of available admin roles that you can assign to user accounts, use this command:

```
Get-MsolRole | Sort Name | Select Name,Description
```


After you determine the Display Name of the account and the name of the role, use these commands to assign the role to the account:

```
$dispName="<The Display Name of the account>"
$roleName="<The admin role name you want to assign to the account>"
Add-MsolRoleMember -RoleMemberEmailAddress (Get-MsolUser -All | Where DisplayName -eq
$dispName).UserPrincipalName -RoleName $roleName
```

Paste the commands into Notepad. For the *\$dispName* and *\$roleName* variables, replace the description text with their values. Remove the < and > characters but keep the quotation marks. Paste the modified lines into the Microsoft Azure Active Directory Module for Windows PowerShell window to run them. Alternately, you can use the Windows PowerShell Integrated Script Environment (ISE).

Here's an example of a completed command set:

```
$dispName="Scott Wallace"
$roleName="SharePoint Service Administrator"
Add-MsolRoleMember -RoleMemberEmailAddress (Get-MsolUser -All | Where DisplayName -eq
$dispName).UserPrincipalName -RoleName $roleName
```

Sign-in names of user accounts

If you're used to working with the sign-in names or UPNs of user accounts, determine the following information:

- The user account's UPN

If you don't know the UPN, use this command:

```
Get-MsolUser -All | Sort UserPrincipalName | Select UserPrincipalName | More
```

This command lists the UPN of your user accounts, sorted by UPN, one screen at a time. You can use the **Where** cmdlet to filter the list. Here's an example:

```
Get-MsolUser -All | Where DisplayName -like "John*" | Sort UserPrincipalName | Select
UserPrincipalName | More
```

This command lists only the user accounts for which the Display Name starts with "John".

- The role you want to assign

To display the list of available roles that you can assign to user accounts, use this command:

```
Get-MsolRole | Sort Name | Select Name,Description
```

After you have the UPN of the account and the name of the role, use these commands to assign the role to the account:

```
$upnName="<The UPN of the account>"
$roleName="<The role name you want to assign to the account>"
Add-MsolRoleMember -RoleMemberEmailAddress $upnName -RoleName $roleName
```

Copy the commands and paste them into Notepad. For the *\$upnName* and *\$roleName* variables. Replace the description text with their values. Remove the < and > characters but keep the quotation marks. Paste the modified lines into Microsoft Azure Active Directory Module for Windows PowerShell window to run them. Alternately, you can use the Windows PowerShell ISE.

Here's an example of a completed command set:

```
$upnName="scottw@contoso.com"
$roleName="SharePoint Service Administrator"
Add-MsolRoleMember -RoleMemberEmailAddress $upnName -RoleName $roleName
```

Multiple role changes

For multiple role changes, determine the following information:

- Which user accounts you want to configure. You can use the methods in the previous section to gather the set of display names or UPNs.
- Which roles you want to assign to each user account. To display the list of available roles that you can assign to user accounts, use this command:

```
Get-MsolRole | Sort Name | Select Name,Description
```

Next, create a comma-separated value (CSV) text file that has the display name or UPN and role name fields. You can do this easily in Microsoft Excel.

Here's an example for display names:

```
DisplayName,RoleName
"Belinda Newman","Billing Administrator"
"Scott Wallace","SharePoint Service Administrator"
```

Next, fill in the location of the CSV file and run the resulting commands at the PowerShell command prompt.

```
$fileName="<path and file name of the input CSV file that has the role changes, example:
C:\admin\RoleUpdates.CSV>"
$roleChanges=Import-Csv $fileName | ForEach {Add-MsolRoleMember -RoleMemberEmailAddress (Get-MsolUser |
Where DisplayName -eq $_.DisplayName).UserPrincipalName -RoleName $_.RoleName }
```

Here's an example for UPNs:

```
UserPrincipalName,RoleName
"belindan@contoso.com","Billing Administrator"
"scottw@contoso.com","SharePoint Service Administrator"
```

Next, fill in the location of the CSV file and run the resulting commands at the PowerShell command prompt.

```
$fileName="<path and file name of the input CSV file that has the role changes, example:
C:\admin\RoleUpdates.CSV>"
$roleChanges=Import-Csv $fileName | ForEach { Add-MsolRoleMember -RoleMemberEmailAddress
$_UserPrincipalName -RoleName $_.RoleName }
```

See also

- [Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)
- [Manage Microsoft 365 with PowerShell](#)
- [Get started with PowerShell for Microsoft 365](#)

Delete Microsoft 365 user accounts with PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

You can use PowerShell for Microsoft 365 to delete and restore user accounts.

NOTE

Learn how to [restore a user account](#) by using the Microsoft 365 admin center.

For a list of additional resources, see [Manage users and groups](#).

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

After you connect, use the following syntax to remove an individual user account:

```
Remove-AzureADUser -ObjectID <sign-in name>
```

This example removes the user account *fabricec@litwareinc.com*.

```
Remove-AzureADUser -ObjectID fabricec@litwareinc.com
```

NOTE

The *-ObjectID* parameter in the **Remove-AzureADUser** cmdlet accepts either the account's sign-in name, also known as the User Principal Name or the account's object ID.

To display the account name based on the user's name, use the following commands:

```
$userName="<User name>"  
Write-Host (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

This example displays the account name for the user *Caleb Sills*.

```
$userName="Caleb Sills"  
Write-Host (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

To remove an account based on the user's display name, use the following commands:

```
$userName="<display name>"  
Remove-AzureADUser -ObjectID (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

When you delete a user account through the Microsoft Azure Active Directory Module for Windows PowerShell,

the account isn't permanently deleted. You can restore the deleted user account within 30 days.

First, [connect to your Microsoft 365 tenant](#).

To delete a user account, use the following syntax:

```
Remove-MsolUser -UserPrincipalName <sign-in name>
```

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with *Mso* in their name. Run these cmdlets from Windows PowerShell.

This example deletes the user account *BelindaN@litwareinc.com*.

```
Remove-MsolUser -UserPrincipalName belindan@litwareinc.com
```

To restore a deleted user account within the 30-day grace period, use the following syntax:

```
Restore-MsolUser -UserPrincipalName <sign-in name>
```

This example restores the deleted account *BelindaN@litwareinc.com*.

```
Restore-MsolUser -UserPrincipalName BelindaN@litwareinc.com
```

NOTE

To see the list of deleted users that can be restored, run the following command:

```
Get-MsolUser -All -ReturnDeletedUsers
```

If the user account's original user principal name is used by another account, use the *NewUserPrincipalName* parameter instead of *UserPrincipalName* to specify a different user principal name when you restore the user account.

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Block Microsoft 365 user accounts with PowerShell

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

When you block access to a Microsoft 365 account, you prevent anyone from using the account to sign in and access the services and data in your Microsoft 365 organization. You can use PowerShell to block access to individual or multiple user accounts.

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

Block access to individual user accounts

Use the following syntax to block an individual user account:

```
Set-AzureADUser -ObjectID <sign-in name of the user account> -AccountEnabled $false
```

NOTE

The *-ObjectID* parameter in the **Set-AzureAD** cmdlet accepts either the account sign-in name, also known as the User Principal Name, or the account's object ID.

This example blocks access to the user account *fabricec@litwareinc.com*.

```
Set-AzureADUser -ObjectID fabricec@litwareinc.com -AccountEnabled $false
```

To unblock this user account, run the following command:

```
Set-AzureADUser -ObjectID fabricec@litwareinc.com -AccountEnabled $true
```

To display the user account UPN based on the user's display name, use the following commands:

```
$userName="<display name>"  
Write-Host (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

This example displays the user account UPN for the user *Caleb Sills*.

```
$userName="Caleb Sills"  
Write-Host (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName
```

To block an account based on the user's display name, use the following commands:

```
$userName="<display name>"
Set-AzureADUser -ObjectID (Get-AzureADUser | where {$_.DisplayName -eq $userName}).UserPrincipalName -
AccountEnabled $false
```

To check the blocked status of a user account use the following command:

```
Get-AzureADUser -ObjectID <UPN of user account> | Select DisplayName,AccountEnabled
```

Block multiple user accounts

To block access for multiple user accounts, create a text file that contains one account sign-in name on each line like this:

```
akol@contoso.com
tjohnston@contoso.com
kakers@contoso.com
```

In the following commands, the example text file is *C:\My Documents\Accounts.txt*. Replace this file name with the path and file name of your text file.

To block access to the accounts listed in the text file, run the following command:

```
Get-Content "C:\My Documents\Accounts.txt" | ForEach {Set-AzureADUser -ObjectID $_ -AccountEnabled $false}
```

To unblock the accounts that are listed in the text file, run the following command:

```
Get-Content "C:\My Documents\Accounts.txt" | ForEach {Set-AzureADUser -ObjectID $_ -AccountEnabled $true}
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

Block individual user accounts

Use the following syntax to block access for an individual user account:

```
Set-MsolUser -UserPrincipalName <sign-in name of user account> -BlockCredential $true
```

NOTE

PowerShell Core doesn't support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets that have *Mso/* in their name. You have to run these cmdlets from Windows PowerShell.

This example blocks access to the user account *fabricec@litwareinc.com*.

```
Set-MsolUser -UserPrincipalName fabricec@litwareinc.com -BlockCredential $true
```

To unblock the user account, run the following command:

```
Set-MsolUser -UserPrincipalName <sign-in name of user account> -BlockCredential $false
```

To check the blocked status of a user account run the following command:

```
Get-MsolUser -UserPrincipalName <sign-in name of user account> | Select DisplayName,BlockCredential
```

Block access for multiple user accounts

First, create a text file that contains one account on each line like this:

```
akol@contoso.com  
tjohnston@contoso.com  
kakers@contoso.com
```

In the following commands, the example text file is *C:\My Documents\Accounts.txt*. Replace this file name with the path and file name of your text file.

To block access for the accounts that are listed in the text file, run the following command:

```
Get-Content "C:\My Documents\Accounts.txt" | ForEach { Set-MsolUser -UserPrincipalName $_ -BlockCredential $true }
```

To unblock the accounts listed in the text file, run the following command:

```
Get-Content "C:\My Documents\Accounts.txt" | ForEach { Set-MsolUser -UserPrincipalName $_ -BlockCredential $false }
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Get started with PowerShell for Microsoft 365](#)

Manage passwords with PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use PowerShell for Microsoft 365 as an alternative to the Microsoft 365 admin center to manage passwords in Microsoft 365.

When a command block in this article requires that you specify variable values, use these steps.

1. Copy the command block to the clipboard and paste it into Notepad or the PowerShell Integrated Script Environment (ISE).
2. Fill in the variable values and remove the "<" and ">" characters.
3. Run the commands in the PowerShell window or the PowerShell ISE.

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

Set a password

Use these commands to specify a password for a user account.

```
$userUPN="<user account sign in name, such as belindan@contoso.com>"
$newPassword="<new password>"
$secPassword = ConvertTo-SecureString $newPassword -AsPlainText -Force
Set-AzureADUserPassword -ObjectId $userUPN -Password $secPassword
```

Force a user to change their password

Use these commands to set a password and force a user to change their new password.

```
$userUPN="<user account sign in name, such as belindan@contoso.com>"
$newPassword="<new password>"
$secPassword = ConvertTo-SecureString $newPassword -AsPlainText -Force
Set-AzureADUserPassword -ObjectId $userUPN -Password $secPassword -EnforceChangePasswordPolicy $true
```

Use these commands to set a password and force a user to change their new password the next time they sign in.

```
$userUPN="<user account sign in name, such as belindan@contoso.com>"
$newPassword="<new password>"
$secPassword = ConvertTo-SecureString $newPassword -AsPlainText -Force
Set-AzureADUserPassword -ObjectId $userUPN -Password $secPassword -ForceChangePasswordNextLogin $true
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

Set a password

Use these commands to specify a password for a user account.


```
$userUPN="<user account sign in name>"  
$newPassword="<new password>"  
Set-MsolUserPassword -UserPrincipalName $userUPN -NewPassword $newPassword
```

Force a user to change their password

Use these commands to force a user to change their password.

```
$userUPN="<user account sign in name>"  
Set-MsolUserPassword -UserPrincipalName $userUPN -ForceChangePassword $true
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

View Microsoft 365 licenses and services with PowerShell

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Every Microsoft 365 subscription consists of the following elements:

- **Licensing plans** These are also known as license plans or Microsoft 365 plans. Licensing plans define the Microsoft 365 services that are available to users. Your Microsoft 365 subscription may contain multiple licensing plans. An example licensing plan would be Microsoft 365 E3.
- **Services** These are also known as service plans. Services are the Microsoft 365 products, features, and capabilities that are available in each licensing plan, for example, Exchange Online and Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus). Users can have multiple licenses assigned to them from different licensing plans that grant access to different services.
- **Licenses** Each licensing plan contains the number of licenses that you purchased. You assign licenses to users so they can use the Microsoft 365 services that are defined by the licensing plan. Every user account requires at least one license from one licensing plan so they can log on to Microsoft 365 and use the services.

You can use PowerShell for Microsoft 365 to view details about the available licensing plans, licenses, and services in your Microsoft 365 organization. For more information about the products, features, and services that are available in different Office 365 subscriptions, see [Office 365 Plan Options](#).

Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Reading subscription license plans requires the `Organization.Read.All` permission scope or one of the other permissions listed in the ['List subscribedSkus' Graph API reference page](#).

```
Connect-Graph -Scopes Organization.Read.All
```

To view summary information about your current licensing plans and the available licenses for each plan, run this command:

```
Get-MgSubscribedSku | Select -Property Sku*, ConsumedUnits -ExpandProperty PrepaidUnits | Format-List
```

The results contain:

- **SkuPartNumber**: Shows the available licensing plans for your organization. For example, `ENTERPRISEPACK` is the license plan name for Office 365 Enterprise E3.
- **Enabled**: Number of licenses that you've purchased for a specific licensing plan.
- **ConsumedUnits**: Number of licenses that you've assigned to users from a specific licensing plan.

To view details about the Microsoft 365 services that are available in all of your license plans, first display a list of your license plans.

```
Get-MgSubscribedSku
```

Next, store the license plans information in a variable.

```
$licenses = Get-MgSubscribedSku
```

Next, display the services in a specific license plan.

```
$licenses[<index>].ServicePlans
```

<index> is an integer that specifies the row number of the license plan from the display of the `Get-MgSubscribedSku | Select SkuPartNumber` command, minus 1.

For example, if the display of the `Get-MgSubscribedSku | Select SkuPartNumber` command is this:

```
SkuPartNumber
-----
WIN10_VDA_E5
EMSPREMIUM
ENTERPRISEPREMIUM
FLOW_FREE
```

Then the command to display the services for the ENTERPRISEPREMIUM license plan is this:

```
$licenses[2].ServicePlans
```

ENTERPRISEPREMIUM is the third row. Therefore, the index value is (3 - 1), or 2.

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#).

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

To view summary information about your current licensing plans and the available licenses for each plan, run this command:

```
Get-AzureADSubscribedSku | Select -Property Sku*,ConsumedUnits -ExpandProperty PrepaidUnits
```

The results contain:

- **SkuPartNumber**: Shows the available licensing plans for your organization. For example, `ENTERPRISEPACK` is the license plan name for Office 365 Enterprise E3.
- **Enabled**: Number of licenses that you've purchased for a specific licensing plan.
- **ConsumedUnits**: Number of licenses that you've assigned to users from a specific licensing plan.

To view details about the Microsoft 365 services that are available in all of your license plans, first display a list of your license plans.

```
Get-AzureADSubscribedSku | Select SkuPartNumber
```

Next, store the license plans information in a variable.

```
$licenses = Get-AzureADSubscribedSku
```

Next, display the services in a specific license plan.

```
$licenses[<index>].ServicePlans
```

<index> is an integer that specifies the row number of the license plan from the display of the `Get-AzureADSubscribedSku | Select SkuPartNumber` command, minus 1.

For example, if the display of the `Get-AzureADSubscribedSku | Select SkuPartNumber` command is this:

```
SkuPartNumber
-----
WIN10_VDA_E5
EMSPREMIUM
ENTERPRISEPREMIUM
FLOW_FREE
```

Then the command to display the services for the ENTERPRISEPREMIUM license plan is this:

```
$licenses[2].ServicePlans
```

ENTERPRISEPREMIUM is the third row. Therefore, the index value is (3 - 1), or 2.

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#).

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

NOTE

A PowerShell script is available that automates the procedures described in this topic. Specifically, the script lets you view and disable services in your Microsoft 365 organization, including Sway. For more information, see [Disable access to Sway with PowerShell](#).

To view summary information about your current licensing plans and the available licenses for each plan, run the following command:

```
Get-MsolAccountSku
```

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

The results contain the following information:

- **AccountSkuId**: Show the available licensing plans for your organization by using the syntax `<CompanyName>:<LicensingPlan>`. *<CompanyName>* is the value that you provided when you enrolled in Microsoft 365, and is unique for your organization. The *<LicensingPlan>* value is the same for everyone. For example, in the value `litwareinc:ENTERPRISEPACK`, the company name is `litwareinc`, and the licensing plan name `ENTERPRISEPACK`, which is the system name for Office 365 Enterprise E3.
- **ActiveUnits**: Number of licenses that you've purchased for a specific licensing plan.
- **WarningUnits**: Number of licenses in a licensing plan that you haven't renewed, and that will expire after the 30-day grace period.
- **ConsumedUnits**: Number of licenses that you've assigned to users from a specific licensing plan.

To view details about the Microsoft 365 services that are available in all of your license plans, run the following command:

```
Get-MsolAccountSku | Select -ExpandProperty ServiceStatus
```

The following table shows the Microsoft 365 service plans and their friendly names for the most common services. Your list of service plans might be different.

SERVICE PLAN	DESCRIPTION
SWAY	Sway
TEAMS1	Microsoft Teams
YAMMER_ENTERPRISE	Yammer
RMS_S_ENTERPRISE	Azure Rights Management (RMS)
OFFICESUBSCRIPTION	Microsoft 365 Apps for enterprise (<i>previously named Office 365 ProPlus</i>)
MCOSTANDARD	Skype for Business Online
SHAREPOINTWAC	Office
SHAREPOINTENTERPRISE	SharePoint Online
EXCHANGE_S_ENTERPRISE	Exchange Online Plan 2

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#).

To view details about the Microsoft 365 services that are available in a specific licensing plan, use the following syntax.

```
(Get-MsolAccountSku | where {$_.AccountSkuId -eq "<AccountSkuId>"}).ServiceStatus
```

This example shows the services that are available in the litwareinc:ENTERPRISEPACK (Office 365 Enterprise E3) licensing plan.

```
(Get-MsolAccountSku | where {$_.AccountSkuId -eq "litwareinc:ENTERPRISEPACK"}).ServiceStatus
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

View licensed and unlicensed Microsoft 365 users with PowerShell

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

User accounts in your Microsoft 365 organization may have some, all, or none of the available licenses assigned to them from the licensing plans that are available in your organization. You can use PowerShell for Microsoft 365 to quickly find the licensed and unlicensed users in your organization.

Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Reading user properties including license details requires the User.Read.All permission scope or one of the other permissions listed in the '[Get a user](#)' [Graph API reference page](#).

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

```
Connect-Graph -Scopes User.Read.All, Organization.Read.All
```

To view the license details of a specific user account, run the following command:

```
Get-MgUserLicenseDetail -UserId "<user sign-in name (UPN)>"
```

For example:

```
Get-MgUserLicenseDetail -UserId "belindan@litwareinc.com"
```

To view the list of all user accounts in your organization that have NOT been assigned any of your licensing plans (unlicensed users), run the following command:

```
Get-MgUser -Filter 'assignedLicenses/$count eq 0' -ConsistencyLevel eventual -CountVariable  
unlicensedUserCount -All  
  
Write-Host "Found $unlicensedUserCount unlicensed users."
```

To view the list of all member user accounts (excluding guests) in your organization that have NOT been assigned any of your licensing plans (unlicensed users), run the following command:

```
Get-MgUser -Filter "assignedLicenses/`$count eq 0 and userType eq 'Member'" -ConsistencyLevel eventual -  
CountVariable unlicensedUserCount -All  
  
Write-Host "Found $unlicensedUserCount unlicensed users (excluding guests)."
```

To view the list of all user accounts in your organization that have been assigned any of your licensing plans (licensed users), run the following command:

```
Get-MgUser -Filter 'assignedLicenses/$count ne 0' -ConsistencyLevel eventual -CountVariable  
licensedUserCount -All -Select UserPrincipalName,DisplayName,AssignedLicenses | Format-Table -Property  
UserPrincipalName,DisplayName,AssignedLicenses  
  
Write-Host "Found $licensedUserCount licensed users."
```

To view the list of all user accounts in your organization that have an E5 license assigned, run the following command:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'  
  
Get-MgUser -Filter "assignedLicenses/any(x:x/skuId eq $($e5Sku.SkuId) )" -ConsistencyLevel eventual -  
CountVariable e5licensedUserCount -All  
  
Write-Host "Found $e5licensedUserCount E5 licensed users."
```

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

To view the list of all user accounts in your organization that have NOT been assigned any of your licensing plans (unlicensed users), run the following command:

```
Get-AzureAdUser | ForEach{ $licensed=$False ; For ($i=0; $i -le ($_.AssignedLicenses | Measure).Count ;  
$i++) { If( [string]::IsNullOrEmpty( $_.AssignedLicenses[$i].SkuId ) -ne $True) { $licensed=$true } } ; If(  
$licensed -eq $false) { Write-Host $_.UserPrincipalName} }
```

To view the list of all user accounts in your organization that have been assigned any of your licensing plans (licensed users), run the following command:

```
Get-AzureAdUser | ForEach { $licensed=$False ; For ($i=0; $i -le ($_.AssignedLicenses | Measure).Count ;  
$i++) { If( [string]::IsNullOrEmpty( $_.AssignedLicenses[$i].SkuId ) -ne $True) { $licensed=$true } } ; If(  
$licensed -eq $true) { Write-Host $_.UserPrincipalName} }
```

NOTE

To list all of the users in your subscription, use the `Get-AzureAdUser -All $true` command.

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

To view the list of all user accounts and their licensing status in your organization, run the following command in PowerShell:

```
Get-MsolUser -All
```


NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

To view the list of all unlicensed user accounts in your organization, run the following command:

```
Get-MsolUser -All -UnlicensedUsersOnly
```

To view the list of all licensed user accounts in your organization, run the following command:

```
Get-MsolUser -All | where {$_.isLicensed -eq $true}
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Assign Microsoft 365 licenses to user accounts with PowerShell

10/28/2022 • 8 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Users can't use any Microsoft 365 services until their account has been assigned a license from a licensing plan. You can use PowerShell to quickly assign licenses to unlicensed accounts.

User accounts must first be assigned a location. Specifying a location is a required part of creating a new user account in the [Microsoft 365 admin center](#).

Accounts synchronized from your on-premises Active Directory Domain Services do not by default have a location specified. You can configure a location for these accounts from:

- The Microsoft 365 admin center
- [PowerShell](#)
- The [Azure portal](#) (Active Directory > Users > user account > Profile > Contact info > Country or region).

NOTE

Learn how to assign licenses to user accounts with the Microsoft 365 admin center. For a list of additional resources, see [Manage users and groups](#).

Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the '[Assign license](#)' [Microsoft Graph API reference page](#).

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

```
Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All
```

Run the `Get-MgSubscribedSku` command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is **ActiveUnits** - **WarningUnits** - **ConsumedUnits**. For more information about licensing plans, licenses, and services, see [View licenses and services with PowerShell](#).

To find the unlicensed accounts in your organization, run this command.

```
Get-MgUser -Filter 'assignedLicenses/$count eq 0' -ConsistencyLevel eventual -CountVariable unlicensedUserCount -All
```

To find the unlicensed synchronized users in your organization, run this command.

```
Get-MgUser -Filter 'assignedLicenses/$count eq 0 and OnPremisesSyncEnabled eq true' -ConsistencyLevel eventual -CountVariable unlicensedUserCount -All -Select UserPrincipalName
```

You can only assign licenses to user accounts that have the **UsageLocation** property set to a valid ISO 3166-1 alpha-2 country code. For example, US for the United States, and FR for France. Some Microsoft 365 services aren't available in certain countries. For more information, see [About license restrictions](#).

To find accounts that don't have a **UsageLocation** value, run this command.

```
Get-MgUser -Select Id,DisplayName,Mail,UserPrincipalName,UsageLocation,UserType | where { $_.UsageLocation -eq $null -and $_.UserType -eq 'Member' }
```

To set the **UsageLocation** value on an account, run this command.

```
$userUPN="<user sign-in name (UPN)>"
$userLoc="<ISO 3166-1 alpha-2 country code>"

Update-MgUser -UserId $userUPN -UsageLocation $userLoc
```

For example:

```
Update-MgUser -UserId "belindan@litwareinc.com" -UsageLocation US
```

If you use the **Get-MgUser** cmdlet without using the **-All** parameter, only the first 100 accounts are returned.

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

```
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} -RemoveLicenses @()
```

This example assigns a license from the **SPE_E5** (Microsoft 365 E5) licensing plan to the unlicensed user **belindan@litwareinc.com**:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId = $e5Sku.SkuId} -RemoveLicenses @()
```

This example assigns **SPE_E5** (Microsoft 365 E5) and **EMSPREMIUM** (ENTERPRISE MOBILITY + SECURITY E5) to the user **belindan@litwareinc.com**:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$e5EmsSku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'EMSPREMIUM'
$addLicenses = @(
    @{SkuId = $e5Sku.SkuId},
    @{SkuId = $e5EmsSku.SkuId}
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses -RemoveLicenses @()
```

This example assigns **SPE_E5** (Microsoft 365 E5) with the **MICROSOFTBOOKINGS** (Microsoft Bookings) and **LOCKBOX_ENTERPRISE** (Customer Lockbox) services turned off:

```

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$disabledPlans = $e5Sku.ServicePlans | `
    Where ServicePlanName -in ("LOCKBOX_ENTERPRISE", "MICROSOFTBOOKINGS") | `
    Select -ExpandProperty ServicePlanId

$addLicenses = @(
    @{
        SkuId = $e5Sku.SkuId
        DisabledPlans = $disabledPlans
    }
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses -RemoveLicenses @()

```

This example updates a user with **SPE_E5** (Microsoft 365 E5) and turns off the Sway and Forms service plans while leaving the user's existing disabled plans in their current state:

```

$userLicense = Get-MgUserLicenseDetail -UserId "belinda@fdoau.onmicrosoft.com"
$userDisabledPlans = $userLicense.ServicePlans | `
    Where ProvisioningStatus -eq "Disabled" | `
    Select -ExpandProperty ServicePlanId

$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$newDisabledPlans = $e5Sku.ServicePlans | `
    Where ServicePlanName -in ("SWAY", "FORMS_PLAN_E5") | `
    Select -ExpandProperty ServicePlanId

$disabledPlans = ($userDisabledPlans + $newDisabledPlans) | Select -Unique

$addLicenses = @(
    @{
        SkuId = $e5Sku.SkuId
        DisabledPlans = $disabledPlans
    }
)

Set-MgUserLicense -UserId "belinda@litwareinc.onmicrosoft.com" -AddLicenses $addLicenses -RemoveLicenses @()

```

Assign licenses to a user by copying the license assignment from another user

This example assigns **jamesp@litwareinc.com** with the same licensing plan that has been applied to **belindan@litwareinc.com**:

```

$mgUser = Get-MgUser -UserId "belindan@litwareinc.com" -Property AssignedLicenses
Set-MgUserLicense -UserId "jamesp@litwareinc.com" -AddLicenses $mgUser.AssignedLicenses -RemoveLicenses @()

```

Move a user to a different subscription (license plan)

This example upgrades a user from the **SPE_E3** (Microsoft 365 E3) licensing plan to the **SPE_E5** (Microsoft 365 E5) licensing plan:

```

$e3Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E3'
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'

# Unassign E3
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{} -RemoveLicenses @($e3Sku.SkuId)
# Assign E5
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId = $e5Sku.SkuId} -RemoveLicenses @()

```

You can verify the change in subscription for the user account with this command.

```
Get-MgUserLicenseDetail -UserId "belindan@litwareinc.com"
```

Use the Azure Active Directory PowerShell for Graph module

NOTE

The Set-AzureADUserLicense cmdlet is scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above. For more information, see [Migrate your apps to access the license managements APIs from Microsoft Graph](#).

First, [connect to your Microsoft 365 tenant](#).

Next, list the license plans for your tenant with this command.

```
Get-AzureADSubscribedSku | Select SkuPartNumber
```

Next, get the sign-in name of the account to which you want to add a license, also known as the user principal name (UPN).

Next, ensure that the user account has a usage location assigned.

```
Get-AzureADUser -ObjectID <user sign-in name (UPN)> | Select DisplayName, UsageLocation
```

If there is no usage location assigned, you can assign one with these commands:

```
$userUPN="<user sign-in name (UPN)>"
$userLoc="<ISO 3166-1 alpha-2 country code>"
Set-AzureADUser -ObjectID $userUPN -UsageLocation $userLoc
```

Finally, specify the user sign-in name and license plan name and run these commands.

```
$userUPN="<user sign-in name (UPN)>"
$planName="<license plan name from the list of license plans>"
$License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$License.SkuId = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value $planName -EQ).SkuID
$LicensesToAssign = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$LicensesToAssign.AddLicenses = $License
Set-AzureADUserLicense -ObjectId $userUPN -AssignedLicenses $LicensesToAssign
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

NOTE

The Set-MsolUserLicense and New-MsolUser (-LicenseAssignment) cmdlets are scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above. For more information, see [Migrate your apps to access the license managements APIs from Microsoft Graph](#).

First, [connect to your Microsoft 365 tenant](#).

Run the `Get-MsolAccountSku` command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is **ActiveUnits - WarningUnits - ConsumedUnits**. For more information about licensing plans, licenses, and services, see [View licenses and services with PowerShell](#).

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

To find the unlicensed accounts in your organization, run this command.

```
Get-MsolUser -All -UnlicensedUsersOnly
```

You can only assign licenses to user accounts that have the **UsageLocation** property set to a valid ISO 3166-1 alpha-2 country code. For example, US for the United States, and FR for France. Some Microsoft 365 services aren't available in certain countries. For more information, see [About license restrictions](#).

To find accounts that don't have a **UsageLocation** value, run this command.

```
Get-MsolUser -All | where {$_.UsageLocation -eq $null}
```

To set the **UsageLocation** value on an account, run this command.

```
Set-MsolUser -UserPrincipalName "<Account>" -UsageLocation <CountryCode>
```

For example:

```
Set-MsolUser -UserPrincipalName "belindan@litwareinc.com" -UsageLocation US
```

If you use the **Get-MsolUser** cmdlet without using the **-All** parameter, only the first 500 accounts are returned.

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

```
Set-MsolUserLicense -UserPrincipalName "<Account>" -AddLicenses "<AccountSkuId>"
```

This example assigns a license from the **litwareinc:ENTERPRISEPACK** (Office 365 Enterprise E3) licensing plan to the unlicensed user **belindan@litwareinc.com**:

```
Set-MsolUserLicense -UserPrincipalName "belindan@litwareinc.com" -AddLicenses "litwareinc:ENTERPRISEPACK"
```

To assign a license to all unlicensed users, run this command.

```
Get-MsolUser -All -UnlicensedUsersOnly [<FilterableAttributes>] | Set-MsolUserLicense -AddLicenses "<AccountSkuId>"
```

NOTE

You can't assign multiple licenses to a user from the same licensing plan. If you don't have enough available licenses, the licenses are assigned to users in the order that they're returned by the **Get-MsolUser** cmdlet until the available licenses run out.

This example assigns licenses from the **litwareinc:ENTERPRISEPACK** (Office 365 Enterprise E3) licensing plan to all unlicensed users:

```
Get-MsolUser -All -UnlicensedUsersOnly | Set-MsolUserLicense -AddLicenses "litwareinc:ENTERPRISEPACK"
```

This example assigns those same licenses to unlicensed users in the Sales department in the United States:

```
Get-MsolUser -All -Department "Sales" -UsageLocation "US" -UnlicensedUsersOnly | Set-MsolUserLicense -AddLicenses "litwareinc:ENTERPRISEPACK"
```

Move a user to a different subscription (license plan) with the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

Next, get the sign-in name of the user account for which you want switch subscriptions, also known as the user principal name (UPN).

Next, list the subscriptions (license plans) for your tenant with this command.

```
Get-AzureADSubscribedSku | Select SkuPartNumber
```

Next, list the subscriptions that the user account currently has with these commands.

```
$userUPN="<user account UPN>"
$licensePlanList = Get-AzureADSubscribedSku
$userList = Get-AzureADUser -ObjectID $userUPN | Select -ExpandProperty AssignedLicenses | Select SkuID
$userList | ForEach { $sku=$_.SkuId ; $licensePlanList | ForEach { If ( $sku -eq
$_.ObjectId.substring($_.ObjectId.length - 36, 36) ) { Write-Host $_.SkuPartNumber } } }
```

Identify the subscription the user currently has (the FROM subscription) and the subscription to which the user is moving (the TO subscription).

Finally, specify the TO and FROM subscription names (SKU part numbers) and run these commands.

```

$subscriptionFrom="<SKU part number of the current subscription>"
$subscriptionTo="<SKU part number of the new subscription>"
# Unassign
$license = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$licenses.RemoveLicenses = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value
$subscriptionFrom -EQ).SkuID
Set-AzureADUserLicense -ObjectId $userUPN -AssignedLicenses $licenses
# Assign
$license.SkuId = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value $subscriptionTo -
EQ).SkuID
$licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$licenses.AddLicenses = $License
Set-AzureADUserLicense -ObjectId $userUPN -AssignedLicenses $licenses

```

You can verify the change in subscription for the user account with these commands.

```

$licensePlanList = Get-AzureADSubscribedSku
$userList = Get-AzureADUser -ObjectId $userUPN | Select -ExpandProperty AssignedLicenses | Select SkuID
$userList | ForEach { $sku=$_.SkuId ; $licensePlanList | ForEach { If ( $sku -eq
$_.ObjectId.substring($_.ObjectId.length - 36, 36) ) { Write-Host $_.SkuPartNumber } } }

```

See also

[Manage user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Use the Microsoft Graph [user: assignLicense](#) and [subscribedSku](#) APIs

View Microsoft 365 account license and service details with PowerShell

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

In Microsoft 365, licenses from licensing plans (also called SKUs or Microsoft 365 plans) give users access to the Microsoft 365 services that are defined for those plans. However, a user might not have access to all the services that are available in a license that's currently assigned to them. You can use PowerShell for Microsoft 365 to view the status of services on user accounts.

For more information about licensing plans, license, and services, see [View licenses and services with PowerShell](#).

Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Reading user properties including license details requires the User.Read.All permission scope or one of the other permissions listed in the ['Get a user' Graph API reference page](#).

```
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All
```

Next, list the license plans for your tenant with this command.

```
Get-MgSubscribedSku
```

Use these commands to list the services that are available in each licensing plan.

```
$allSKUs = Get-MgSubscribedSku -Property SkuPartNumber, ServicePlans
$allSKUs | ForEach-Object {
    Write-Host "Service Plan:" $_.SkuPartNumber
    $_.ServicePlans | ForEach-Object {$_}
}
```

Use these commands to list the licenses that are assigned to a user account.

```
Get-MgUserLicenseDetail -UserId "<user sign-in name (UPN)>"
```

For example:

```
Get-MgUserLicenseDetail -UserId "belindan@litwareinc.com"
```

To view services for a user account

To view all the Microsoft 365 services that a user has access to, use the following syntax:

```
(Get-MgUserLicenseDetail -UserId <user account UPN> -Property ServicePlans)
[<LicenseIndexNumber>].ServicePlans
```

This example shows the services to which the user BelindaN@litwareinc.com has access. This shows the services that are associated with all licenses that are assigned to her account.

```
(Get-MgUserLicenseDetail -UserId belindan@litwareinc.com -Property ServicePlans).ServicePlans
```

This example shows the services that user BelindaN@litwareinc.com has access to from the first license that's assigned to her account (the index number is 0).

```
(Get-MgUserLicenseDetail -UserId belindan@litwareinc.com -Property ServicePlans)[0].ServicePlans
```

To view all the services for a user who has been assigned *multiple licenses*, use the following syntax:

```
$userUPN="<user account UPN>"
$allLicenses = Get-MgUserLicenseDetail -UserId $userUPN -Property SkuPartNumber, ServicePlans
$allLicenses | ForEach-Object {
    Write-Host "License:" $_.SkuPartNumber
    $_.ServicePlans | ForEach-Object {$_}
}
```

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

Next, list the license plans for your tenant with this command.

```
Get-AzureADSubscribedSku | Select SkuPartNumber
```

Use these commands to list the services that are available in each licensing plan.

```
$allSKUs=Get-AzureADSubscribedSku
$licArray = @()
for($i = 0; $i -lt $allSKUs.Count; $i++)
{
    $licArray += "Service Plan: " + $allSKUs[$i].SkuPartNumber
    $licArray += Get-AzureADSubscribedSku -ObjectID $allSKUs[$i].ObjectID | Select -ExpandProperty ServicePlans
    $licArray += ""
}
$licArray
```

Use these commands to list the licenses that are assigned to a user account.

```
$userUPN="<user account UPN, such as belindan@contoso.com>"
$licensePlanList = Get-AzureADSubscribedSku
$userList = Get-AzureADUser -ObjectID $userUPN | Select -ExpandProperty AssignedLicenses | Select SkuID
$userList | ForEach { $sku=$_.SkuId ; $licensePlanList | ForEach { If ( $sku -eq
$_.Objectid.substring($_.Objectid.length - 36, 36) ) { Write-Host $_.SkuPartNumber } } }
```

Use the Microsoft Azure Active Directory Module for Windows

PowerShell

First, [connect to your Microsoft 365 tenant](#).

Next, run this command to list the licensing plans that are available in your organization.

```
Get-MsolAccountSku
```

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

Next, run this command to list the services that are available in each licensing plan, and the order in which they are listed (the index number).

```
(Get-MsolAccountSku | where {$_.AccountSkuId -eq "<AccountSkuId>"}).ServiceStatus
```

Use this command to list the licenses that are assigned to a user, and the order in which they are listed (the index number).

```
Get-MsolUser -UserPrincipalName <user account UPN> | Format-List DisplayName,Licenses
```

To view services for a user account

To view all the Microsoft 365 services that a user has access to, use the following syntax:

```
(Get-MsolUser -UserPrincipalName <user account UPN>).Licenses[<LicenseIndexNumber>].ServiceStatus
```

This example shows the services to which the user BelindaN@litwareinc.com has access. This shows the services that are associated with all licenses that are assigned to her account.

```
(Get-MsolUser -UserPrincipalName belindan@litwareinc.com).Licenses.ServiceStatus
```

This example shows the services that user BelindaN@litwareinc.com has access to from the first license that's assigned to her account (the index number is 0).

```
(Get-MsolUser -UserPrincipalName belindan@litwareinc.com).Licenses[0].ServiceStatus
```

To view all the services for a user who has been assigned *multiple licenses*, use the following syntax:

```
$userUPN="<user account UPN>"
$AllLicenses=(Get-MsolUser -UserPrincipalName $userUPN).Licenses
$licArray = @()
for($i = 0; $i -lt $AllLicenses.Count; $i++)
{
    $licArray += "License: " + $AllLicenses[$i].AccountSkuId
    $licArray += $AllLicenses[$i].ServiceStatus
    $licArray += "
"
}
$licArray
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Remove Microsoft 365 licenses from user accounts with PowerShell

10/28/2022 • 4 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

NOTE

Learn how to remove licenses from user accounts with the Microsoft 365 admin center. For a list of additional resources, see [Manage users and groups](#).

Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the ['Assign license' Graph API reference page](#).

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

```
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All
```

To view the licensing plan information in your organization, see the following topics:

- [View licenses and services with PowerShell](#)
- [View account license and service details with PowerShell](#)

Removing licenses from user accounts

To remove licenses from an existing user account, use the following syntax:

```
Set-MgUserLicense -UserId "<Account>" -RemoveLicenses @"(<AccountSkuId1>)" -AddLicenses @{}
```

This example removes the SPE_E5 (Microsoft 365 E5) licensing plan from the user

BelindaN@litwareinc.com:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'  
Set-MgUserLicense -UserId "belindan@litwareinc.com" -RemoveLicenses @($e5Sku.SkuId) -AddLicenses @{}
```

To remove all licenses from a group of existing licensed users, use the following syntax:

```
$licensedUsers = Get-MgUser -Filter 'assignedLicenses/$count ne 0' `
    -ConsistencyLevel eventual -CountVariable licensedUserCount -All `
    -Select UserPrincipalName,DisplayName,AssignedLicenses

foreach($user in $licensedUsers)
{
    $licencesToRemove = $user.AssignedLicenses | Select -ExpandProperty SkuId
    $user = Set-MgUserLicense -UserId $user.UserPrincipalName -RemoveLicenses $licencesToRemove -AddLicenses
    @{}
}
```

Another way to free up a license is by deleting the user account. For more information, see [Delete and restore user accounts with PowerShell](#).

Use the Azure Active Directory PowerShell for Graph module

The Set-AzureADUserLicense cmdlet is scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above. For more information, see [Migrate your apps to access the license managements APIs from Microsoft Graph](#).

First, [connect to your Microsoft 365 tenant](#).

Next, list the license plans for your tenant with this command.

```
Get-AzureADSubscribedSku | Select SkuPartNumber
```

Next, get the sign-in name of the account for which you want to remove a license, also known as the user principal name (UPN).

Finally, specify the user sign-in and license plan names, remove the "<" and ">" characters, and run these commands.

```
$userUPN="<user sign-in name (UPN)>"
$planName="<license plan name from the list of license plans>"
$license = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$license.RemoveLicenses = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value $planName
-EQ).SkuID
Set-AzureADUserLicense -ObjectId $userUPN -AssignedLicenses $license
```

To remove all of the licenses for a specific user account, specify the user sign-in name, remove the "<" and ">" characters, and run these commands.

```

$userUPN="<user sign-in name (UPN)>"
$userList = Get-AzureADUser -ObjectID $userUPN
$Skus = $userList | Select -ExpandProperty AssignedLicenses | Select SkuID
if($userList.Count -ne 0) {
    if($Skus -is [array])
    {
        $licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
        for ($i=0; $i -lt $Skus.Count; $i++) {
            $licenses.RemoveLicenses += (Get-AzureADSubscribedSku | Where-Object -Property SkuID -Value
$Skus[$i].SkuId -EQ).SkuID
        }
        Set-AzureADUserLicense -ObjectID $userUPN -AssignedLicenses $licenses
    } else {
        $licenses = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
        $licenses.RemoveLicenses = (Get-AzureADSubscribedSku | Where-Object -Property SkuID -Value
$Skus.SkuId -EQ).SkuID
        Set-AzureADUserLicense -ObjectID $userUPN -AssignedLicenses $licenses
    }
}

```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

NOTE

The Set-MsolUserLicense and New-MsolUser (-LicenseAssignment) cmdlets are scheduled to be retired. Please migrate your scripts to the Microsoft Graph SDK's Set-MgUserLicense cmdlet as described above. For more information, see [Migrate your apps to access the license managements APIs from Microsoft Graph](#).

First, [connect to your Microsoft 365 tenant](#).

To view the licensing plan (**AccountSkuID**) information in your organization, see the following topics:

- [View licenses and services with PowerShell](#)
- [View account license and service details with PowerShell](#)

If you use the **Get-MsolUser** cmdlet without using the **-All** parameter, only the first 500 accounts are returned.

Removing licenses from user accounts

To remove licenses from an existing user account, use the following syntax:

```
Set-MsolUserLicense -UserPrincipalName <Account> -RemoveLicenses "<AccountSkuId1>", "<AccountSkuId2>"...
```

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

This example removes the **litwareinc:ENTERPRISEPACK** (Office 365 Enterprise E3) license from the user account BelindaN@litwareinc.com.

```
Set-MsolUserLicense -UserPrincipalName belindan@litwareinc.com -RemoveLicenses "litwareinc:ENTERPRISEPACK"
```

NOTE

You cannot use the `Set-MsolUserLicense` cmdlet to unassign users from *canceled* licenses. You must do this individually for each user account in the Microsoft 365 admin center.

To remove all licenses from a group of existing licensed users, use either of the following methods:

- **Filter the accounts based on an existing account attribute** To do this, use the following syntax:

```
$userArray = Get-MsolUser -All <FilterableAttributes> | where {$_.isLicensed -eq $true}
for ($i=0; $i -lt $userArray.Count; $i++)
{
    Set-MsolUserLicense -UserPrincipalName $userArray[$i].UserPrincipalName -RemoveLicenses
    $userArray[$i].licenses.accountskuid
}
```

This example removes all licenses from all user accounts in the Sales department in the United States.

```
$userArray = Get-MsolUser -All -Department "Sales" -UsageLocation "US" | where {$_.isLicensed -eq $true}
for ($i=0; $i -lt $userArray.Count; $i++)
{
    Set-MsolUserLicense -UserPrincipalName $userArray[$i].UserPrincipalName -RemoveLicenses
    $userArray[$i].licenses.accountskuid
}
```

- **Use a list of specific accounts for a specific license** To do this, perform the following steps:

1. Create and save a text file that contains one account on each line like this:

```
akol@contoso.com
tjohnston@contoso.com
kakers@contoso.com
```

2. Use the following syntax:

```
$x=Get-Content "<FileNameAndPath>"
for ($i=0; $i -lt $x.Count; $i++)
{
    Set-MsolUserLicense -UserPrincipalName $x[$i] -RemoveLicenses "<AccountSkuId1>","<AccountSkuId2>"...
}
```

This example removes the **litwareinc:ENTERPRISEPACK** (Office 365 Enterprise E3) license from the user accounts defined in the text file C:\My Documents\Accounts.txt.

```
$x=Get-Content "C:\My Documents\Accounts.txt"
for ($i=0; $i -lt $x.Count; $i++)
{
    Set-MsolUserLicense -UserPrincipalName $x[$i] -RemoveLicenses "litwareinc:ENTERPRISEPACK"
}
```

To remove all licenses from all existing user accounts, use the following syntax:


```
$userArray = Get-MsolUser -All | where {$_.islicensed -eq $true}
for ($i=0; $i -lt $userArray.Count; $i++)
{
    Set-MsolUserLicense -UserPrincipalName $userArray[$i].UserPrincipalName -RemoveLicenses
    $userArray[$i].licenses.accounts
}
```

Another way to free up a license is by deleting the user account. For more information, see [Delete and restore user accounts with PowerShell](#).

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Disable access to Microsoft 365 services with PowerShell

10/28/2022 • 7 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

When a Microsoft 365 account is assigned a license from a licensing plan, Microsoft 365 services are made available to the user from that license. However, you can control the Microsoft 365 services that the user can access. For example, even though the license allows access to the SharePoint Online service, you can disable access to it. You can use PowerShell to disable access to any number of services for a specific licensing plan for:

- An individual account.
- A group of accounts.
- All accounts in your organization.

NOTE

There are Microsoft 365 service dependencies that can prevent you from disabling a specified service when other services depend on it.

Use the Microsoft Graph PowerShell SDK

First, [connect to your Microsoft 365 tenant](#).

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the ['Assign license' Graph API reference page](#).

The Organization.Read.All permission scope is required to read the licenses available in the tenant.

```
Connect-Graph -Scopes User.ReadWrite.All, Organization.Read.All
```

Next, use this command to view your available licensing plans, also known as SkuPartNumber:

```
Get-MgSubscribedSku | Select SkuId, SkuPartNumber, ServicePlans | Sort SkuPartNumber
```

For more information, see [View licenses and services with PowerShell](#).

To see the before and after results of the procedures in this topic, see [View account license and service details with PowerShell](#).

Disable specific Microsoft 365 services for specific users for a specific licensing plan

To disable a specific set of Microsoft 365 services for users for a specific licensing plan, perform the following steps:

Step 1: Identify the undesired services in the licensing plan by using the following syntax:

First list the licensing plans available in your tenant using the following command.

```
Get-MgSubscribedSku | Select SkuPartNumber
```

```
SkuPartNumber
-----
EMSPREMIUM
SPE_E5
RIGHTSMANAGEMENT_ADHOC
```

Next, use the SkuPartNumber from the command above, list the service plans available for a given license plan (Sku).

The following example lists all the service plans available for **SPE_E5** (Microsoft 365 E5).

```
Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5' | select -ExpandProperty ServicePlans
```

AppliesTo	ProvisioningStatus	ServicePlanId	ServicePlanName
-----	-----	-----	-----
User	Success	b21a6b06-1988-436e-a07b-51ec6d9f52ad	PROJECT_0365_P3
User	Success	64bfac92-2b17-4482-b5e5-a0304429de3e	MICROSOFTENDPOINTDLP
User	Success	199a5c09-e0ca-4e37-8f7c-b05d533e1ea2	MICROSOFTBOOKINGS
User	Success	6db1f1db-2b46-403f-be40-e39395f08dbb	CUSTOMER_KEY
User	Success	4a51bca5-1eff-43f5-878c-177680f191af	WHITEBOARD_PLAN3
User	Success	07699545-9485-468e-95b6-2fca3738be01	FLOW_0365_P3
User	Success	9c0dab89-a30c-4117-86e7-97bda240acd2	POWERAPPS_0365_P3
User	Success	e212cbc7-0961-4c40-9825-01117710dcb1	FORMS_PLAN_E5
User	Success	57ff2da0-773e-42df-b2af-ffb7a2317929	TEAMS1
User	Success	21b439ba-a0ca-424f-a6cc-52f954a5b111	WIN10_PRO_ENT_SUB
User	Success	eec0eb4f-6444-4f95-aba0-50c24d67f998	AAD_PREMIUM_P2
User	Success	c1ec4a95-1f05-45b3-a911-aa3fa01094f5	INTUNE_A
User	Success	7547a3fe-08ee-4ccb-b430-5077c5041653	YAMMER_ENTERPRISE
User	Success	a23b959c-7ce8-4e57-9140-b90eb88a9e97	SWAY
User	Success	e95bec33-7c88-4a70-8e19-b10bd9d0c014	SHAREPOINTWAC
User	Success	5dbe027f-2339-4123-9542-606e4d348a72	SHAREPOINTENTERPRISE
User	Success	b737dad2-2f6c-4c65-90e3-ca563267e8b9	PROJECTWORKMANAGEMENT
User	Success	43de0ff5-c92c-492b-9116-175376d08c38	OFFICESUBSCRIPTION
User	Success	0feae32-d00e-4d66-bd5a-43b5b83db82c	MCSTANDARD
User	Success	9f431833-0334-42de-a7dc-70aa40db46db	LOCKBOX_ENTERPRISE
User	Success	efb87545-963c-4e0d-99df-69c6916d9eb0	EXCHANGE_S_ENTERPRISE

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#). (Search using the ServicePlanId to lookup service plan's corresponding friendly name).

The following example assigns **SPE_E5** (Microsoft 365 E5) with the **MICROSOFTBOOKINGS** (Microsoft Bookings) and **LOCKBOX_ENTERPRISE** (Customer Lockbox) services turned off:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$disabledPlans = $e5Sku.ServicePlans | `
    Where ServicePlanName -in ("LOCKBOX_ENTERPRISE", "MICROSOFTBOOKINGS") | `
    Select -ExpandProperty ServicePlanId

$addLicenses = @(
    @{
        SkuId = $e5Sku.SkuId
        DisabledPlans = $disabledPlans
    }
)

Set-MgUserLicense -UserId "belinda@litwareinc.com" -AddLicenses $addLicenses -RemoveLicenses @()
```

The DisabledPlans property of the AddLicenses parameter in Set-MgUserLicense will overwrite the user's existing DisabledPlans value. To preserve the state of existing service plans, the user's current state of service plans must be merged with the new plans that are going to be disabled.

Failing to include the existing DisabledPlans will result in the user's previously disabled plan being enabled.

The following example updates a user with **SPE_E5** (Microsoft 365 E5) and turns off the Sway and Forms service plans while leaving the user's existing disabled plans in their current state:

```
## Get the services that have already been disabled for the user.
$userLicense = Get-MgUserLicenseDetail -UserId "belinda@fdoau.onmicrosoft.com"
$userDisabledPlans = $userLicense.ServicePlans | `
    Where ProvisioningStatus -eq "Disabled" | `
    Select -ExpandProperty ServicePlanId

## Get the new service plans that are going to be disabled
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
$newDisabledPlans = $e5Sku.ServicePlans | `
    Where ServicePlanName -in ("SWAY", "FORMS_PLAN_E5") | `
    Select -ExpandProperty ServicePlanId

## Merge the new plans that are to be disabled with the user's current state of disabled plans
$disabledPlans = ($userDisabledPlans + $newDisabledPlans) | Select -Unique

$addLicenses = @(
    @{
        SkuId = $e5Sku.SkuId
        DisabledPlans = $disabledPlans
    }
)

## Update user's license
Set-MgUserLicense -UserId "belinda@litwareinc.onmicrosoft.com" -AddLicenses $addLicenses -RemoveLicenses @()
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

Next, use this command to view your available licensing plans, also known as AccountSkulds:

```
Get-MsolAccountSku | Select AccountSkuId | Sort AccountSkuId
```

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

For more information, see [View licenses and services with PowerShell](#).

To see the before and after results of the procedures in this topic, see [View account license and service details with PowerShell](#).

A PowerShell script is available that automates the procedures described in this topic. Specifically, the script lets you view and disable services in your Microsoft 365 organization, including Sway. For more information, see [Disable access to Sway with PowerShell](#).

Disable specific Microsoft 365 services for specific users for a specific licensing plan

To disable a specific set of Microsoft 365 services for users for a specific licensing plan, perform the following

steps:

Step 1: Identify the undesired services in the licensing plan by using the following syntax:

```
$LO = New-MsolLicenseOptions -AccountSkuId <AccountSkuId> -DisabledPlans "<UndesiredService1>", "  
<UndesiredService2>"...
```

The following example creates a **LicenseOptions** object that disables the Office and SharePoint Online services in the licensing plan named `litwareinc:ENTERPRISEPACK` (Office 365 Enterprise E3).

```
$LO = New-MsolLicenseOptions -AccountSkuId "litwareinc:ENTERPRISEPACK" -DisabledPlans "SHAREPOINTWAC",  
"SHAREPOINTENTERPRISE"
```

Step 2: Use the LicenseOptions object from Step 1 on one or more users.

To create a new account that has the services disabled, use the following syntax:

```
New-MsolUser -UserPrincipalName <Account> -DisplayName <DisplayName> -FirstName <FirstName> -LastName  
<LastName> -LicenseAssignment <AccountSkuId> -LicenseOptions $LO -UsageLocation <CountryCode>
```

The following example creates a new account for Allie Bellew that assigns the license and disables the services described in Step 1.

```
New-MsolUser -UserPrincipalName allieb@litwareinc.com -DisplayName "Allie Bellew" -FirstName Allie -LastName  
Bellew -LicenseAssignment litwareinc:ENTERPRISEPACK -LicenseOptions $LO -UsageLocation US
```

For more information about creating user accounts in PowerShell for Microsoft 365, see [Create user accounts with PowerShell](#).

To disable the services for an existing licensed user, use the following syntax:

```
Set-MsolUserLicense -UserPrincipalName <Account> -LicenseOptions $LO
```

This example disables the services for the user BelindaN@litwareinc.com.

```
Set-MsolUserLicense -UserPrincipalName belindan@litwareinc.com -LicenseOptions $LO
```

To disable the services described in Step 1 for all existing licensed users, specify the name of your Microsoft 365 plan from the display of the **Get-MsolAccountSku** cmdlet (such as `litwareinc:ENTERPRISEPACK`), and then run the following commands:

```
$acctSKU="<AccountSkuId>"  
$AllLicensed = Get-MsolUser -All | Where {$_.isLicensed -eq $true -and $_.licenses.AccountSku.SkuPartNumber  
-contains ($acctSKU).Substring($acctSKU.IndexOf(":")+1, $acctSKU.Length-$acctSKU.IndexOf(":")-1)}  
$AllLicensed | ForEach {Set-MsolUserLicense -UserPrincipalName $_.UserPrincipalName -LicenseOptions $LO}
```

If you use the **Get-MsolUser** cmdlet without using the *All* parameter, only the first 500 user accounts are returned.

To disable the services for a group of existing users, use either of the following methods to identify the users:

Method 1. Filter the accounts based on an existing account attribute

To do this, use the following syntax:

```
$x = Get-MsolUser -All <FilterableAttributes>
$x | ForEach {Set-MsolUserLicense -UserPrincipalName $_.UserPrincipalName -LicenseOptions $LO}
```

The following example disables the services for users in the Sales department in the United States.

```
$USSales = Get-MsolUser -All -Department "Sales" -UsageLocation "US"
$USSales | ForEach {Set-MsolUserLicense -UserPrincipalName $_.UserPrincipalName -LicenseOptions $LO}
```

Method 2: Use a list of specific accounts

To do this, perform the following steps:

1. Create a text file that contains one account on each line like this:

```
akol@contoso.com
tjohnston@contoso.com
kakers@contoso.com
```

In this example, the text file is C:\My Documents\Accounts.txt.

2. Run the following command:

```
Get-Content "C:\My Documents\Accounts.txt" | foreach {Set-MsolUserLicense -UserPrincipalName $_ -
LicenseOptions $LO}
```

If you want to disable access to services for multiple licensing plans, repeat the above instructions for each licensing plan, ensuring that:

- The user accounts have been assigned the licensing plan.
- The services to disable are available in the licensing plan.

To disable Microsoft 365 services for users while you are assigning them to a licensing plan, see [Disable access to services while assigning user licenses](#).

Assign all services in a licensing plan to a user account

For user accounts that have had services disabled, you can enable all services for a specific licensing plan with these commands:

```
$userUPN="<user account UPN>"
$acctSKU="<AccountSkuId>"
$LO = New-MsolLicenseOptions -AccountSkuId $acctSKU
Set-MsolUserLicense -UserPrincipalName $userUPN -LicenseOptions $LO
```

Related topic

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Disable access to Sway with PowerShell for Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

The ManageSway.ps1 PowerShell script lets you view and disable services in your Microsoft 365 organization, including Sway. This script automates the procedures that are described in the following topics:

- [View licenses and services with PowerShell](#)
- [Disable access to services with PowerShell](#)

You need to download the two files that are associated with the script:

- The ManageSway.ps1 script at <https://go.microsoft.com/fwlink/p/?LinkId=785070>
- The help file for the script at <https://go.microsoft.com/fwlink/p/?LinkId=785072>

Disable access to Microsoft 365 services while assigning user licenses

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Microsoft 365 subscriptions come with service plans for individual services. Microsoft 365 administrators often need to disable certain plans when assigning licenses to users. With the instructions in this article, you can assign a Microsoft 365 license while disabling specific service plans using PowerShell for an individual user account or multiple user accounts.

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

Next, list the license plans for your tenant with this command.

```
Get-AzureADSubscribedSku | Select SkuPartNumber
```

Next, get the sign-in name of the account to which you want add a license, also known as the user principal name (UPN).

Next, compile a list of services to enable. For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#).

For the command block below, fill in the user principal name of the user account, the SKU part number, and the list of service plans to enable and remove the explanatory text and the < and > characters. Then, run the resulting commands at the PowerShell command prompt.

```
$userUPN="<user account UPN>"
$skuPart="<SKU part number>"
$serviceList=<double-quoted enclosed, comma-separated list of enabled services>
$user = Get-AzureADUser -ObjectId $userUPN
$skuID = (Get-AzureADSubscribedSku | Where {$_.SkuPartNumber -eq $skuPart}).SkuID
$skuFeaturesToEnable = @($serviceList)
$StandardLicense = Get-AzureADSubscribedSku | Where {$_.SkuId -eq $skuID}
$SkuFeaturesToDisable = $StandardLicense.ServicePlans | ForEach-Object { $_ | Where {$_.ServicePlanName -notin $SkuFeaturesToEnable }}
$License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$License.SkuId = $StandardLicense.SkuId
$License.DisabledPlans = $SkuFeaturesToDisable.ServicePlanId
$LicensesToAssign = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$LicensesToAssign.AddLicenses = $License
Set-AzureADUserLicense -ObjectId $user.ObjectId -AssignedLicenses $LicensesToAssign
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

Next, run this command to see your current subscriptions:


```
Get-MsolAccountSku
```

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

In the display of the `Get-MsolAccountSku` command:

- **AccountSkuId** is a subscription for your organization in <OrganizationName>:<Subscription> format. The <OrganizationName> is the value that you provided when you enrolled in Microsoft 365, and is unique for your organization. The <Subscription> value is for a specific subscription. For example, for litwareinc:ENTERPRISEPACK, the organization name is litwareinc, and the subscription name is ENTERPRISEPACK (Office 365 Enterprise E3).
- **ActiveUnits** is the number of licenses that you've purchased for the subscription.
- **WarningUnits** is the number of licenses in a subscription that you haven't renewed, and that will expire after the 30-day grace period.
- **ConsumedUnits** is the number of licenses that you've assigned to users for the subscription.

Note the AccountSkuId for your Microsoft 365 subscription that contains the users you want to license. Also, ensure that there are enough licenses to assign (subtract **ConsumedUnits** from **ActiveUnits**).

Next, run this command to see the details about the Microsoft 365 service plans that are available in all your subscriptions:

```
Get-MsolAccountSku | Select -ExpandProperty ServiceStatus
```

From the display of this command, determine which service plans you would like to disable when you assign licenses to users.

Here is a partial list of service plans and their corresponding Microsoft 365 services.

The following table shows the Microsoft 365 service plans and their friendly names for the most common services. Your list of service plans might be different.

SERVICE PLAN	DESCRIPTION
<code>SWAY</code>	Sway
<code>TEAMS1</code>	Microsoft Teams
<code>YAMMER_ENTERPRISE</code>	Yammer
<code>RMS_S_ENTERPRISE</code>	Azure Rights Management (RMS)
<code>OFFICESUBSCRIPTION</code>	Microsoft 365 Apps for enterprise (<i>previously named Office 365 ProPlus</i>)
<code>MCOSTANDARD</code>	Skype for Business Online

SERVICE PLAN	DESCRIPTION
SHAREPOINTWAC	Office
SHAREPOINTENTERPRISE	SharePoint Online
EXCHANGE_S_ENTERPRISE	Exchange Online Plan 2

For a complete list of license plans (also known as product names), their included service plans, and their corresponding friendly names, see [Product names and service plan identifiers for licensing](#).

Now that you have the AccountSkuId and the service plans to disable, you can assign licenses for an individual user or for multiple users.

For a single user

For a single user, fill in the user principal name of the user account, the AccountSkuId, and the list of service plans to disable and remove the explanatory text and the < and > characters. Then, run the resulting commands at the PowerShell command prompt.

```
$userUPN="<the user's account name in email format>"
$accountSkuId="<the AccountSkuId from the Get-MsolAccountSku command>"
$planList=@( <comma-separated, double-quote enclosed list of the service plans to disable> )
$licenseOptions=New-MsolLicenseOptions -AccountSkuId $accountSkuId -DisabledPlans $planList
Set-MsolUserLicense -UserPrincipalName $userUpn -AddLicenses $accountSkuId -ErrorAction SilentlyContinue
Sleep -Seconds 5
Set-MsolUserLicense -UserPrincipalName $userUpn -LicenseOptions $licenseOptions -ErrorAction
SilentlyContinue
```

Here is an example command block for the account named belindan@contoso.com, for the contoso:ENTERPRISEPACK license, and the service plans to disable are RMS_S_ENTERPRISE, SWAY, INTUNE_O365, and YAMMER_ENTERPRISE:

```
$userUPN="belindan@contoso.com"
$accountSkuId="contoso:ENTERPRISEPACK"
$planList=@( "RMS_S_ENTERPRISE", "SWAY", "INTUNE_O365", "YAMMER_ENTERPRISE" )
$licenseOptions=New-MsolLicenseOptions -AccountSkuId $accountSkuId -DisabledPlans $planList
Set-MsolUserLicense -UserPrincipalName $userUpn -AddLicenses $accountSkuId -ErrorAction SilentlyContinue
Sleep -Seconds 5
Set-MsolUserLicense -UserPrincipalName $userUpn -LicenseOptions $licenseOptions -ErrorAction
SilentlyContinue
```

For multiple users

To perform this administration task for multiple users, create a comma-separated value (CSV) text file that contains the UserPrincipalName and UsageLocation fields. Here is an example:

```
UserPrincipalName,UsageLocation
ClaudeL@contoso.onmicrosoft.com,FR
LynneB@contoso.onmicrosoft.com,US
ShawnM@contoso.onmicrosoft.com,US
```

Next, fill in the location of the input and output CSV files, the account SKU ID, and the list of service plans to disable, and then run the resulting commands at the PowerShell command prompt.

```

$inFileName="<path and file name of the input CSV file that contains the users, example:
C:\admin\Users2License.CSV>"
$outFileName="<path and file name of the output CSV file that records the results, example:
C:\admin\Users2License-Done.CSV>"
$accountSkuId="<the AccountSkuId from the Get-MsolAccountSku command>"
$planList=@( <comma-separated, double-quote enclosed list of the plans to disable> )
$users=Import-Csv $inFileName
$licenseOptions=New-MsolLicenseOptions -AccountSkuId $accountSkuId -DisabledPlans $planList
ForEach ($user in $users)
{
    $user.Userprincipalname
    $upn=$user.UserPrincipalName
    Set-MsolUserLicense -UserPrincipalName $upn -AddLicenses $accountSkuId -ErrorAction SilentlyContinue
    sleep -Seconds 5
    Set-MsolUserLicense -UserPrincipalName $upn -LicenseOptions $licenseOptions -ErrorAction SilentlyContinue
    $users | Get-MsolUser | Select UserPrincipalName, Islicensed,Usagelocation | Export-Csv $outFileName
}

```

This PowerShell command block:

- Displays the user principal name of each user.
- Assigns customized licenses to each user.
- Creates a CSV file with all the users that were processed and shows their license status.

See also

[Disable access to Microsoft 365 services with PowerShell](#)

[Disable access to Sway with PowerShell](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

Manage security groups with PowerShell

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use PowerShell for Microsoft 365 as an alternative to the Microsoft 365 admin center to manage security groups.

This article describes listing, creating, changing settings, and removing security groups.

When a command block in this article requires that you specify variable values, use these steps.

1. Copy the command block to the clipboard and paste it into Notepad or the PowerShell Integrated Script Environment (ISE).
2. Fill in the variable values and remove the "<" and ">" characters.
3. Run the commands in the PowerShell window or the PowerShell ISE.

See [Maintain security group membership](#) to manage group membership with PowerShell.

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

List your groups

Use this command to list all of your groups.

```
Get-AzureADGroup
```

Use these commands to display the settings of a specific group by its display name.

```
$groupName="<display name of the group>"  
Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }
```

Create a new group

Use this command to create a new security group.

```
New-AzureADGroup -Description "<group purpose>" -DisplayName "<name>" -MailEnabled $false -SecurityEnabled $true -MailNickName "<email name>"
```

Change the settings on a group

Display the settings of the group with these commands.

```
$groupName="<display name of the group>"  
Get-AzureADGroup | Where { $_.DisplayName -eq $groupName } | Select *
```

Then, use the [Set-AzureADGroup](#) article to determine how to change a setting.

Remove a security group

Use these commands to remove a security group.

```
$groupName="<display name of the group>"
Remove-AzureADGroup -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId
```

Manage the owners of a security group

Use these commands to display the current owners of a security group.

```
$groupName="<display name of the group>"
Get-AzureADGroupOwner -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId
```

Use these commands to add a user account by its **user principal name (UPN)** to the current owners of a security group.

```
$userUPN="<UPN of the user account to add>"
$groupName="<display name of the group>"
Add-AzureADGroupOwner -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId -
RefObjectId (Get-AzureADUser | Where { $_.UserPrincipalName -eq $userUPN }).ObjectId
```

Use these commands to add a user account by its **display name** to the current owners of a security group.

```
$userName="<Display name of the user account to add>"
$groupName="<display name of the group>"
Add-AzureADGroupOwner -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId -
RefObjectId (Get-AzureADUser | Where { $_.DisplayName -eq $userName }).ObjectId
```

Use these commands to remove a user account by its **UPN** to the current owners of a security group.

```
$userUPN="<UPN of the user account to remove>"
$groupName="<display name of the group>"
Remove-AzureADGroupOwner -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId -
OwnerId (Get-AzureADUser | Where { $_.UserPrincipalName -eq $userUPN }).ObjectId
```

Use these commands to remove a user account by its **display name** to the current owners of a security group.

```
$userName="<Display name of the user account to remove>"
$groupName="<display name of the group>"
Remove-AzureADGroupOwner -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId -
OwnerId (Get-AzureADUser | Where { $_.DisplayName -eq $userName }).ObjectId
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

List your groups

Use this command to list all of your groups.

```
Get-MsolGroup
```

Use these commands to display the settings of a specific group by its display name.

```
$groupName="<display name of the group>"
Get-MsolGroup | Where { $_.DisplayName -eq $groupName }
```

Create a new group

Use this command to create a new security group.

```
New-MsolGroup -Description "<group purpose>" -DisplayName "<name>"
```

Change the settings on a group

Display the settings of the group with these commands.

```
$groupName="<display name of the group>"
Get-MsolGroup | Where { $_.DisplayName -eq $groupName } | Select *
```

Then, use the [Set-MsolGroup](#) article to determine how to change a setting.

Remove a security group

Use these commands to remove a security group.

```
$groupName="<display name of the group>"
Remove-MsolGroup -ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectId
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Maintain security group membership with PowerShell

10/28/2022 • 5 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can use PowerShell for Microsoft 365 as an alternative to the Microsoft 365 admin center to maintain security group membership in Microsoft 365.

NOTE

Learn how to maintain Microsoft 365 group membership with the Microsoft 365 admin center. For a list of additional resources, see [Manage users and groups](#).

Use the Azure Active Directory PowerShell for Graph module

First, [connect to your Microsoft 365 tenant](#).

Add or remove user accounts as members of a group

To add a user account by its UPN, fill in the user account User Principal Name (UPN) (example: belindan@contoso.com) and the security group display name, removing the "<" and ">" characters, and run these commands in the PowerShell window or the PowerShell Integrated Script Environment (ISE).

```
$userUPN="<UPN of the user account to add>"
$groupName="<display name of the group>"
Add-AzureADGroupMember -RefObjectId (Get-AzureADUser | Where { $_.UserPrincipalName -eq $userUPN }).ObjectID -
-ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

To add a user account by its display name, fill in the user account display name (example: Belinda Newman) and the group display name and run these commands in the PowerShell window or the PowerShell ISE.

```
$userName="<display name of the user account to add>"
$groupName="<display name of the group>"
Add-AzureADGroupMember -RefObjectId (Get-AzureADUser | Where { $_.DisplayName -eq $userName }).ObjectID -
-ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

To remove a user account by its UPN, fill in the user account UPN (example: belindan@contoso.com) and the group display name and run these commands in the PowerShell window or the PowerShell ISE.

```
$userUPN="<UPN of the user account to remove>"
$groupName="<display name of the group>"
Remove-AzureADGroupMember -MemberId (Get-AzureADUser | Where { $_.UserPrincipalName -eq $userUPN }).ObjectID -
-ObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

To remove a user account by its display name, fill in the user account display name (example: Belinda Newman) and the group display name and run these commands in the PowerShell window or the PowerShell ISE.

```
$userName="<display name of the user account to remove>"
$groupName="<display name of the group>"
Remove-AzureADGroupMember -MemberId (Get-AzureADUser | Where { $_.DisplayName -eq $userName }).ObjectID -
ObjectID (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

Add or remove groups as members of a group

Security groups can contain other groups as members. Microsoft 365 groups, however, cannot. This section contains PowerShell commands to add or remove groups only for a security group.

To add a group by its display name, fill in the display name of the group you're going to add and the display name of the group that will contain the member group and run these commands in the PowerShell window or the PowerShell ISE.

```
$groupMemberName="<display name of the group to add>"
$groupName="<display name of the group that will contain the member group>"
Add-AzureADGroupMember -RefObjectId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupMemberName
}).ObjectID -ObjectID (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

To remove a group by its display name, fill in the display name of the group you're going to remove and the display name of the group that will contain the member group and run these commands in the PowerShell window or the PowerShell ISE.

```
$groupMemberName="<display name of the group to add>"
$groupName="<display name of the group that will contain the member group>"
Remove-AzureADGroupMember -MemberId (Get-AzureADGroup | Where { $_.DisplayName -eq $groupMemberName
}).ObjectID -ObjectID (Get-AzureADGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

Use the Microsoft Azure Active Directory Module for Windows PowerShell

First, [connect to your Microsoft 365 tenant](#).

Add or remove user accounts as members of a group

To add a user account by its UPN, fill in the user account User Principal Name (UPN) (example: belindan@contoso.com) and the group display name, removing the "<" and ">" characters, and run these commands in the PowerShell window or the PowerShell ISE.

```
$userUPN="<UPN of the user account to add>"
$groupName="<display name of the group>"
Add-MsolGroupMember -GroupMemberObjectId (Get-MsolUser | Where { $_.UserPrincipalName -eq $userUPN
}).ObjectID -GroupObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

To add a user account by its display name, fill in the user account display name (example: Belinda Newman) and the group display name and run these commands in the PowerShell window or the PowerShell ISE.

```
$userName="<display name of the user account to add>"
$groupName="<display name of the group>"
Add-MsolGroupMember -GroupMemberObjectId (Get-MsolUser | Where { $_.DisplayName -eq $userName }).ObjectID -
GroupObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupName }).ObjectID
```

To remove a user account by its UPN, fill in the user account UPN (example: belindan@contoso.com) and the group display name and run these commands in the PowerShell window or the PowerShell ISE.


```
$userUPN="<UPN of the user account to remove>"
$groupName="<display name of the group>"
Remove-MsolGroupMember -GroupMemberObjectId (Get-MsolUser | Where { $_.UserPrincipalName -eq $userUPN
}).ObjectId -GroupObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupName }).ObjectId
```

To remove a user account by its display name, fill in the user account display name (example: Belinda Newman) and the group display name and run these commands in the PowerShell window or the PowerShell ISE.

```
$userName="<display name of the user account to remove>"
$groupName="<display name of the group>"
Remove-MsolGroupMember -GroupMemberObjectId (Get-MsolUser | Where { $_.DisplayName -eq $userName }).ObjectId
-GroupObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupName }).ObjectId
```

Add or remove groups as members of a group

Security groups can contain other groups as members. Microsoft 365 groups, however, cannot. This section contains PowerShell commands to add or remove groups only for a security group.

To add a group by its display name, fill in the display name of the group you're going to add and the display name of the group that will contain the member group and run these commands in the PowerShell window or the PowerShell ISE.

```
$groupMemberName="<display name of the group to add>"
$groupName="<display name of the group that will contain the member group>"
Add-MsolGroupMember -GroupMemberObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupMemberName
}).ObjectId -GroupObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupName }).ObjectId -
GroupMemberType Group
```

To remove a group by its display name, fill in the display name of the group you're going to remove and the display name of the group that will contain the member group and run these commands in the PowerShell window or the PowerShell ISE.

```
$groupMemberName="<display name of the group to add>"
$groupName="<display name of the group contains the member group>"
Remove-MsolGroupMember -GroupMemberObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupMemberName
}).ObjectId -GroupObjectId (Get-MsolGroup | Where { $_.DisplayName -eq $groupName }).ObjectId -
GroupMemberType Group
```

See also

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Manage Microsoft 365 Groups with PowerShell

10/28/2022 • 6 minutes to read • [Edit Online](#)

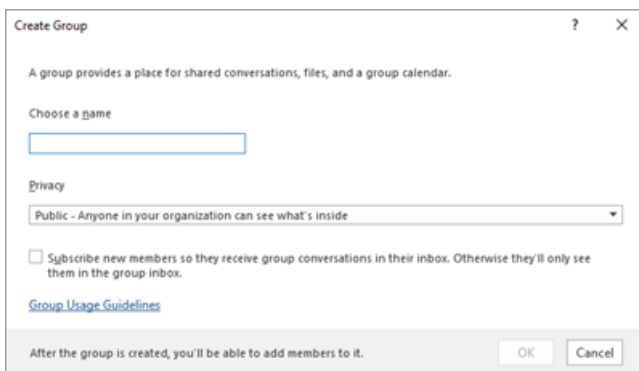
This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

This article provides the steps for doing common management tasks for Groups in Microsoft PowerShell. It also lists the PowerShell cmdlets for Groups. For info about managing SharePoint sites, see [Manage SharePoint Online sites using PowerShell](#).

Link to your Microsoft 365 Groups usage guidelines

When users [create or edit a group in Outlook](#), you can show them a link to your organization's usage guidelines. For example, if you require a specific prefix or suffix to be added to a group name.

Use the Azure Active Directory (Azure AD) PowerShell to point your users to your organization's usage guidelines for Microsoft 365 groups. Check out [Azure Active Directory cmdlets for configuring group settings](#) and follow the steps in the **Create settings at the directory level** to define the usage guideline hyperlink. Once you run the AAD cmdlet, users will see the link to your guidelines when they create or edit a group in Outlook.



Create Group

A group provides a place for shared conversations, files, and a group calendar.

Choose a name

Privacy

Public - Anyone in your organization can see what's inside

☐ Subscribe new members so they receive group conversations in their inbox. Otherwise they'll only see them in the group inbox.

[Group Usage Guidelines](#)

After the group is created, you'll be able to add members to it.

OK Cancel

Save X Discard

Edit group

Group usage guidelines

Name

Description

Privacy

Language for group-related notifications

☐ Let people outside the organization email the group

☐ Subscribe new members so they receive group conversations in their inbox

Allow users to Send as the Microsoft 365 Group

If you want to enable your Microsoft 365 groups to "Send As", use the [Add-RecipientPermission](#) and [Get-RecipientPermission](#) cmdlets to configure this. Once you enable this setting, Microsoft 365 group users can use Outlook or Outlook on the web to send and reply to email as the Microsoft 365 group. Users can go to the group, create a new email, and change the "Send As" field to the group's email address.

(You can also do this in the [Exchange Admin Center](#).)

Use the following script, replacing *<GroupAlias>* with the alias of the group that you want to update, and *<UserAlias>* with the alias of the user to whom you want to grant permissions. [Connect to Exchange Online PowerShell](#) to run this script.

```
$groupAlias = "<GroupAlias>"
$userAlias = "<UserAlias>"
$groupsRecipientDetails = Get-Recipient -RecipientTypeDetails groupmailbox -Identity $groupAlias

Add-RecipientPermission -Identity $groupsRecipientDetails.Name -Trustee $userAlias -AccessRights SendAs
```

Once the cmdlet is executed, users can go to Outlook or Outlook on the web to send as the group, by adding the group email address to the **From** field.

Create classifications for Microsoft 365 Groups in your organization

You can create sensitivity labels that the users in your organization can set when they create a Microsoft 365 Group. If you want to classify groups, we recommend using sensitivity labels instead of the previous groups classification feature. For information about using sensitivity labels, see [Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites](#).

IMPORTANT

If you are currently using classification labels, they will no longer be available to users who create groups once sensitivity labels are enabled.

You can still use the previous groups classification feature. You can create classifications that the users in your organization can set when they create a Microsoft 365 Group. For example, you can allow users to set "Standard", "Secret", and "Top Secret" on groups they create. Group classifications aren't set by default and you need to create it in order for your users to set it. Use Azure Active Directory PowerShell to point your users to your organization's usage guidelines for Microsoft 365 Groups.

Check out [Azure Active Directory cmdlets for configuring group settings](#) and follow the steps in the **Create settings at the directory level** to define the classification for Microsoft 365 Groups.

```
$setting["ClassificationList"] = "Low Impact, Medium Impact, High Impact"
```

In order to associate a description to each classification, you can use the settings attribute *ClassificationDescriptions* to define.

```
$setting["ClassificationDescriptions"] = "Classification:Description,Classification:Description"
```

Where Classification matches the strings in the ClassificationList.

Example:

```
$setting["ClassificationDescriptions"] = "Low Impact: General communication, Medium Impact: Company internal data , High Impact: Data that has regulatory requirements"
```

After you run the above Azure Active Directory cmdlet to set your classification, run the [Set-UnifiedGroup](#) cmdlet if you want to set the classification for a specific group.

```
Set-UnifiedGroup <LowImpactGroup@constoso.com> -Classification <LowImpact>
```

Or create a new group with a classification.

```
New-UnifiedGroup <HighImpactGroup@constoso.com> -Classification <HighImpact> -AccessType <Public>
```

Check out [Using PowerShell with Exchange Online](#) and [Connect to Exchange Online PowerShell](#) for more details on using Exchange Online PowerShell.

Once these settings are enabled, the group owner will be able to choose a classification from the drop down menu in Outlook on the Web and Outlook, and save it from the **Edit** group page.

Save Discard

Edit group

Group usage guidelines

Name
Test Create Group Messages

Description
Test Create Group Messages

Privacy
Private - Only approved members can see what's inside

Classification
Low Impact

- Low Impact
- Medium Impact
- High Impact

Hide Microsoft 365 Groups from the global address list.

You can specify whether a Microsoft 365 Group appears in the global address list (GAL) and other lists in your organization. For example, if you have a legal department group that you don't want to show up in the address list, you can stop that group from appearing in the GAL. Run the Set-Unified Group cmdlet to hide the group from the address list like this:

```
Set-UnifiedGroup -Identity "Legal Department" -HiddenFromAddressListsEnabled $true
```

Allow only internal users to send message to Microsoft 365 Groups

If you don't want users from other organizations to send emails to a Microsoft 365 Group, you can change the settings for that group. It will allow only internal users to send an email to your group. If an external user tries to send a message to that group, it will be rejected.

Run the Set-UnifiedGroup cmdlet to update this setting, like this:

```
Set-UnifiedGroup -Identity "Internal senders only" -RequireSenderAuthenticationEnabled $true
```

Add MailTips to Microsoft 365 Groups

Whenever a sender tries to send an email to a Microsoft 365 Group, a MailTip can be shown to them.

Run the Set-Unified Group cmdlet to add a mailTip to the group:

```
Set-UnifiedGroup -Identity "MailTip Group" -MailTip "This group has a MailTip"
```

Along with MailTip, you can also set MailTipTranslations, which specify other languages for the MailTip. Suppose

you want to have the Spanish translation, then run the following command:

```
Set-UnifiedGroup -Identity "MailaTip Group" -MailTip "This group has a MailTip" -MailTipTranslations
"@{Add="ES:Esta caja no se supervisa."
```

Change the display name of the Microsoft 365 Group

The display name specifies the name of the Microsoft 365 Group. You can see this name in your [Exchange admin center](#) or [Microsoft 365 admin center](#). You can edit the display name of the group or assign a display name to an existing Microsoft 365 Group by running the Set-UnifiedGroup command:

```
Set-UnifiedGroup -Identity "mygroup@contoso.com" -DisplayName "My new group"
```

Change the default setting of Microsoft 365 Groups for Outlook to Public or Private

Microsoft 365 Groups in Outlook are created as Private by default. If your organization wants Microsoft 365 Groups to be created as Public by default (or back to Private), use this PowerShell cmdlet syntax:

```
Set-OrganizationConfig -DefaultGroupAccessType Public
```

To set to Private:

```
Set-OrganizationConfig -DefaultGroupAccessType Private
```

To verify the setting:

```
Get-OrganizationConfig | ft DefaultGroupAccessType
```

To learn more, see [Set-OrganizationConfig](#) and [Get-OrganizationConfig](#).

Microsoft 365 Groups cmdlets

The following cmdlets can be used with Microsoft 365 Groups.

CMDLET NAME	DESCRIPTION
Get-UnifiedGroup	Use this cmdlet to look up existing Microsoft 365 Groups, and to view properties of the group object
Set-UnifiedGroup	Update the properties of a specific Microsoft 365 Group
New-UnifiedGroup	Create a new Microsoft 365 Group. This cmdlet provides a minimal set of parameters. To set values for extended properties, use Set-UnifiedGroup after creating the new group
Remove-UnifiedGroup	Delete an existing Microsoft 365 Group

CMDLET NAME	DESCRIPTION
Get-UnifiedGroupLinks	Retrieve membership and owner information for a Microsoft 365 Group
Add-UnifiedGroupLinks	Add members, owners, and subscribers to an existing Microsoft 365 Group
Remove-UnifiedGroupLinks	Remove owners and members from an existing Microsoft 365 Group
Get-UserPhoto	Used to view information about the user photo associated with an account. User photos are stored in Active Directory
Set-UserPhoto	Used to associate a user photo with an account. User photos are stored in Active Directory
Remove-UserPhoto	Remove the photo for a Microsoft 365 Group

Related topics

[Upgrade distribution lists to Microsoft 365 Groups](#)

[Manage who can create Microsoft 365 Groups](#)

[Manage guest access to Microsoft 365 Groups](#)

[Change static group membership to dynamic in](#)

Manage Folders and Rules feature in Microsoft 365 Groups

10/28/2022 • 2 minutes to read • [Edit Online](#)

Users can organize groups emails effectively by creating folders and setting rules inside groups mailbox. Once the folders are created in groups mailbox, users can move and copy messages to different folders manually as well as using **Rules**.

This capability is currently available only in Outlook Web Application.

Enable Folders and Rules feature for Microsoft 365 Groups in Outlook

Admin can enable the feature with the help of cmdlet `Set-OrganizationConfig -IsGroupFoldersAndRulesEnabled`.

- `[-IsGroupFoldersAndRulesEnabled<Boolean>]` - optional

The `IsGroupFoldersAndRulesEnabled` parameter specifies whether Folders and Rules feature is enabled for the tenant.

Possible values: true/false

Default Value: false

NOTE

Once the `IsGroupFoldersAndRulesEnabled` parameter is turned off after creating some folder and rules,

- Existing Folders and Rules will keep getting rendered.
- Existing rules will keep on executing.
- Folder Creation/Updation/Deletion will be blocked.
- Message level actions Copy/Move will be blocked.

Once the feature is enabled, by default only owner of the group has the permission to create folder, rename folder, move and copy messages across folders.

Enable member permission option

If there's a need for members in the group to create folders and triage messages in groups mailbox, then member permission to edit groups content has to be enabled by the admin at tenant level and group owner at group level respectively.

By default, this setting is set **off** at tenant level and group level

Admin can enable the member permission to the tenant using the cmdlet `IsGroupMemberAllowedToEditContent`.

- `[-IsGroupMemberAllowedToEditContent<Boolean>]` - optional

The `IsGroupMemberAllowedToEditContent` parameter specifies whether group owner can grant permission to members for Folders and Rules feature content edit.

Possible values: True/False

Default value: false

Once this is enabled, Group owners can provide group members with the ability to create folders, rename folders, copy, move and delete messages. Group level member permission is handled by Group owners.

NOTE

Admins can see the current value of the settings using `Get-OrganizationConfig` cmdlet.

Block "Move" message capability

Admins can block the **Move** message option for all Microsoft 365 groups within a tenant using the cmdlet

```
Set-OrganizationConfig -BlockMoveMessagesForGroupFold .
```

- `[-BlockMoveMessagesForGroupFolders<Boolean>]` – optional

The `BlockMoveMessagesForGroupFolders` parameter specifies whether message the **Move** action is disabled.

Possible values: True/False

Default value: false

NOTE

Creation of **Move** rule is also disabled when `BlockMoveMessagesForGroupFolders` is enabled.

NOTE

This is useful if there are mixed set of users using Outlook on Web and Outlook Desktop App. For users on Outlook Desktop App where folders are not available, they can get the messages from group inbox.

Manage SharePoint with PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

SharePoint administrators have to manage sites, site groups, and users. Although you can do some of these tasks in the Microsoft 365 admin center, others are easier in PowerShell. For more information, see the following articles:

- [Get started with SharePoint Online Management Shell](#)
- [Create SharePoint online sites and add users with PowerShell](#)
- [Manage SharePoint online users and groups with PowerShell](#)
- [Manage SharePoint online site groups with PowerShell](#)

See also

- [Manage Microsoft 365 with PowerShell](#)
- [Get started with PowerShell for Microsoft 365](#)

Create SharePoint Online sites and add users with PowerShell

10/28/2022 • 4 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

When you use PowerShell for Microsoft 365 to create SharePoint Online sites and add users, you can quickly and repeatedly perform tasks much faster than you can in the Microsoft 365 admin center. You can also perform tasks that are not possible to perform in the Microsoft 365 admin center.

Connect to SharePoint Online

The procedures in this topic require you to connect to SharePoint Online. For instructions, see [Connect to SharePoint Online PowerShell](#)

Step 1: Create new site collections using PowerShell

Create multiple sites using PowerShell and a .csv file that you create using the example code provided and Notepad. For this procedure, you'll be replacing the placeholder information shown in brackets with your own site- and tenant-specific information. This process lets you create a single file and run a single PowerShell command that uses that file. This makes the actions taken both repeatable and portable and eliminates many, if not all, errors that can come from typing long commands into the SharePoint Online Management Shell. There are two parts to this procedure. First you'll create a .csv file, and then you'll reference that .csv file using PowerShell, which will use its contents to create the sites.

The PowerShell cmdlet imports the .csv file and pipes it to a loop inside the curly brackets that reads the first line of the file as column headers. The PowerShell cmdlet then iterates through the remaining records, creates a new site collection for each record, and assigns properties of the site collection according to the column headers.

Create a .csv file

NOTE

The resource quota parameter works only on classic sites. If you use this parameter on a modern site, you may receive a warning message that it has been deprecated.

1. Open Notepad, and paste the following text block into it:

```
Owner,StorageQuota,Url,ResourceQuota,Template,TimeZoneID,Name
owner@tenant.onmicrosoft.com,100,https://tenant.sharepoint.com/sites/TeamSite01,25,EHS#1,10,Contoso
Team Site
owner@tenant.onmicrosoft.com,100,https://tenant.sharepoint.com/sites/Blog01,25,BLOG#0,10,Contoso Blog
owner@tenant.onmicrosoft.com,150,https://tenant.sharepoint.com/sites/Project01,25,PROJECTSITE#0,10,Project Alpha
owner@tenant.onmicrosoft.com,150,https://tenant.sharepoint.com/sites/Community01,25,COMMUNITY#0,10,Community Site
```

Where *tenant* is the name of your tenant, and *owner* is the user name of the user on your tenant to whom you want to grant the role of primary site collection administrator.

(You can press Ctrl+H when you use Notepad to bulk replace faster.)

2. Save the file on your desktop as **SiteCollections.csv**.

TIP

Before you use this or any other .csv or Windows PowerShell script file, it's a good practice to make sure that there are no extraneous or nonprinting characters. Open the file in Word, and in the ribbon, click the paragraph icon to show nonprinting characters. There should be no extraneous nonprinting characters. For example, there should be no paragraph marks beyond the final one at the end of the file.

Run the Windows PowerShell command

1. At the Windows PowerShell prompt, type or copy and paste the following command, and press Enter:

```
Import-Csv C:\users\MyAlias\desktop\SiteCollections.csv | ForEach-Object {New-SPOSite -Owner $_.Owner  
-StorageQuota $_.StorageQuota -Url $_.Url -NoWait -ResourceQuota $_.ResourceQuota -Template  
$_Template -TimeZoneID $_.TimeZoneID -Title $_.Name}
```

Where *MyAlias* equals your user alias.

2. Wait for the Windows PowerShell prompt to reappear. It might take a minute or two.
3. At the Windows PowerShell prompt, type or copy and paste the following cmdlet, and press Enter:

```
Get-SPOSite -Detailed | Format-Table -AutoSize
```

4. Note the new site collections in the list. Using our example CSV file, you would see the following site collections: **TeamSite01**, **Blog01**, **Project01**, and **Community01**

That's it. You've created multiple site collections using the .csv file you created and a single Windows PowerShell command. You're now ready to create and assign users to these sites.

Step 2: Add users and groups

Now you're going to create users and add them to a site collection group. You will then use a .csv file to bulk upload new groups and users.

The following procedures continue using the example sites TeamSite01, Blog01, Project01, and Community01.

Create .csv and .ps1 files

1. Open Notepad, and paste the following text block into it:

```
Site,Group,PermissionLevels  
https://tenant.sharepoint.com/sites/Community01,Contoso Project Leads,Full Control  
https://tenant.sharepoint.com/sites/Community01,Contoso Auditors,View Only  
https://tenant.sharepoint.com/sites/Community01,Contoso Designers,Design  
https://tenant.sharepoint.com/sites/TeamSite01,XT1000 Team Leads,Full Control  
https://tenant.sharepoint.com/sites/TeamSite01,XT1000 Advisors,Edit  
https://tenant.sharepoint.com/sites/Blog01,Contoso Blog Designers,Design  
https://tenant.sharepoint.com/sites/Blog01,Contoso Blog Editors,Edit  
https://tenant.sharepoint.com/sites/Project01,Project Alpha Approvers,Full Control
```

Where *tenant* equals your tenant name.

2. Save the file to your desktop as **GroupsAndPermissions.csv**.
3. Open a new instance of Notepad, and paste the following text block into it:

```
Group,LoginName,Site
Contoso Project Leads,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Community01
Contoso Auditors,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Community01
Contoso Designers,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Community01
XT1000 Team Leads,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/TeamSite01
XT1000 Advisors,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/TeamSite01
Contoso Blog Designers,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Blog01
Contoso Blog Editors,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Blog01
Project Alpha Approvers,username@tenant.onmicrosoft.com,https://tenant.sharepoint.com/sites/Project01
```

Where *tenant* equals your tenant name, and *username* equals the user name of an existing user.

4. Save the file to your desktop as **Users.csv**.
5. Open a new instance of Notepad, and paste the following text block into it:

```
Import-Csv C:\users\MyAlias\desktop\GroupsAndPermissions.csv | ForEach-Object {New-SPOSiteGroup -
Group $_.Group -PermissionLevels $_.PermissionLevels -Site $_.Site}
Import-Csv C:\users\MyAlias\desktop\Users.csv | where {Add-SPOUser -Group $_.Group -LoginName
$_.LoginName -Site $_.Site}
```

Where MyAlias equals the user name of the user that is currently logged on.

6. Save the file to your desktop as **UsersAndGroups.ps1**. This is a simple Windows PowerShell script.

You're now ready to run the UsersAndGroup.ps1 script to add users and groups to multiple site collections.

Run UsersAndGroups.ps1 script

1. Return to the SharePoint Online Management Shell.
2. At the Windows PowerShell prompt, type or copy and paste the following line, and press Enter:

```
Set-ExecutionPolicy Bypass
```

3. At the confirmation prompt, press **Y**.
4. At the Windows PowerShell prompt, type or copy and paste the following, and press Enter:

```
c:\users\MyAlias\desktop\UsersAndGroups.ps1
```

Where *MyAlias* equals your user name.

5. Wait for the prompt to return before moving on. You will first see the groups appear as they are created. Then you will see the group list repeated as users are added.

See also

[Connect to SharePoint Online PowerShell](#)

[Manage SharePoint Online site groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Manage SharePoint Online users and groups with PowerShell

10/28/2022 • 7 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

If you're a SharePoint Online administrator who works with large lists of user accounts or groups and wants an easier way to manage them, you can use PowerShell for Microsoft 365.

Before you begin, the procedures in this article require you to connect to SharePoint Online. For instructions, see [Connect to SharePoint Online PowerShell](#)

Get a list of sites, groups, and users

Before we start to manage users and groups, you need to get lists of your sites, groups, and users. You can then use this information to work through the example in this article.

Get a list of the sites in your tenant with this command:

```
Get-SPOSite
```

Get a list of the groups in your tenant with this command:

```
Get-SPOSite | ForEach {Get-SPOSiteGroup -Site $_.Url} | Format-Table
```

Get a list of the users in your tenant with this command:

```
Get-SPOSite | ForEach {Get-SPOUser -Site $_.Url}
```

Add a user to the Site Collection Administrators group

You use the `Set-SPOUser` cmdlet to add a user to the list of Site Collection Administrators on a site collection.

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$user = "<user account name, such as opalc>"
Set-SPOUser -Site https://$tenant.sharepoint.com/sites/$site -LoginName $user@$tenant.com -
IsSiteCollectionAdmin $true
```

To use these commands, replace everything within the quotes, including the < and > characters, with the correct names.

For example, this set of commands adds Opal Castillo (user name opalc) to the list of Site Collection Administrators on the ContosoTest site collection in the Contoso tenancy:

```
$tenant = "contoso"
$site = "contosotest"
$user = "opalc"
Set-SPOUser -Site https://$tenant.sharepoint.com/sites/$site -LoginName $user@$tenant.com -
IsSiteCollectionAdmin $true
```

You can copy and paste these commands into Notepad, change the variable values for \$tenant, \$site, and \$user to actual values from your environment, and then paste this into your SharePoint Online Management Shell window to run them.

Add a user to other site collection groups

In this task, we'll use the `Add-SPOUser` cmdlet to add a user to a SharePoint group on a site collection.

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$user = "<user account name, such as opalc>"
$group = "<group name name, such as Auditors>"
Add-SPOUser -Group $group -LoginName $user@$tenant.com -Site https://$tenant.sharepoint.com/sites/$site
```

For example, let's add Glen Rife (user name glennr) to the Auditors group on the ContosoTest site collection in the contoso tenancy:

```
$tenant = "contoso"
$site = "contosotest"
$user = "glennr"
$group = "Auditors"
Add-SPOUser -Group $group -LoginName $user@$tenant.com -Site https://$tenant.sharepoint.com/sites/$site
```

Create a site collection group

You use the `New-SPOSiteGroup` cmdlet to create a new SharePoint group and add it to a site collection.

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$group = "<group name name, such as Auditors>"
$level = "<permission level, such as View Only>"
New-SPOSiteGroup -Group $group -PermissionLevels $level -Site https://$tenant.sharepoint.com/sites/$site
```

Group properties, such as permission levels, can be updated later by using the `Set-SPOSiteGroup` cmdlet.

For example, let's add the Auditors group with View Only permissions to the contosotest site collection in the contoso tenancy:

```
$tenant = "contoso"
$site = "contosotest"
$group = "Auditors"
$level = "View Only"
New-SPOSiteGroup -Group $group -PermissionLevels $level -Site https://$tenant.sharepoint.com/sites/$site
```

Remove users from a group

Sometimes you have to remove a user from a site or even all sites. Perhaps the employee moves from one

division to another or leaves the company. You can do this for one employee easily in the UI, but this isn't easily done when you have to move a complete division from one site to another.

However by using the SharePoint Online Management Shell and CSV files, this is fast and easy. In this task, you'll use Windows PowerShell to remove a user from a site collection security group. Then you'll use a CSV file and remove lots of users from different sites.

We'll be using the 'Remove-SPOUser' cmdlet to remove a single Microsoft 365 user from a site collection group so we can see the command syntax. Here's how the syntax looks:

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
$user = "<user account name, such as opalc>"
$group = "<group name name, such as Auditors>"
Remove-SPOUser -LoginName $user@$tenant.com -Site https://$tenant.sharepoint.com/sites/$site -Group $group
```

For example, let's remove Bobby Overby from the site collection Auditors group in the contosotest site collection in the contoso tenancy:

```
$tenant = "contoso"
$site = "contosotest"
$user = "bobbyo"
$group = "Auditors"
Remove-SPOUser -LoginName $user@$tenant.com -Site https://$tenant.sharepoint.com/sites/$site -Group $group
```

Suppose we wanted to remove Bobby from all the groups he's currently in. Here's how we would do that:

```
$tenant = "contoso"
$user = "bobbyo"
Get-SPOSite | ForEach {Get-SPOSiteGroup -Site $_.Url} | ForEach {Remove-SPOUser -LoginName $user@$tenant.com -Site $_.Url}
```

WARNING

This is just an example. You should not run this command unless you really have to remove a user from every group, for example if the user leaves the company.

Automate management of large lists of users and groups

To add a large number of accounts to SharePoint sites and give them permissions, you can use the Microsoft 365 admin center, individual PowerShell commands, or PowerShell and a CSV file. Of these choices, the CSV file is the fastest way to automate this task.

The basic process is to create a CSV file that has headers (columns) that correspond to the parameters that the Windows PowerShell script needs. You can easily create such a list in Excel and then export it as a CSV file. Then, you use a Windows PowerShell script to iterate through records (rows) in the CSV file, adding the users to groups and the groups to sites.

For example, let's create a CSV file to define a group of site collections, groups, and permissions. Next, we'll create a CSV file to populate the groups with users. Finally, we'll create and run a Windows PowerShell script that creates and populates the groups.

The first CSV file will add one or more groups to one or more site collections and will have this structure:

Header:


```
Site,Group,PermissionLevels
```

Item:

```
https://tenant.sharepoint.com/sites/site,group,level
```

Here's an example file:

```
Site,Group,PermissionLevels
https://contoso.sharepoint.com/sites/contosotest,Contoso Project Leads,Full Control
https://contoso.sharepoint.com/sites/contosotest,Contoso Auditors,View Only
https://contoso.sharepoint.com/sites/contosotest,Contoso Designers,Design
https://contoso.sharepoint.com/sites/TeamSite01,XT1000 Team Leads,Full Control
https://contoso.sharepoint.com/sites/TeamSite01,XT1000 Advisors,Edit
https://contoso.sharepoint.com/sites/Blog01,Contoso Blog Designers,Design
https://contoso.sharepoint.com/sites/Blog01,Contoso Blog Editors,Edit
https://contoso.sharepoint.com/sites/Project01,Project Alpha Approvers,Full Control
```

The second CSV file will add one or more users to one or more groups and will have this structure:

Header:

```
Group,LoginName,Site
```

Item:

```
group,login,https://tenant.sharepoint.com/sites/site
```

Here's an example file:

```
Group,LoginName,Site
Contoso Project Leads,bobbyo@contoso.com,https://contoso.sharepoint.com/sites/contosotest
Contoso Auditors,allieb@contoso.com,https://contoso.sharepoint.com/sites/contosotest
Contoso Designers,bonniek@contoso.com,https://contoso.sharepoint.com/sites/contosotest
XT1000 Team Leads,dorenap@contoso.com,https://contoso.sharepoint.com/sites/TeamSite01
XT1000 Advisors,garthf@contoso.com,https://contoso.sharepoint.com/sites/TeamSite01
Contoso Blog Designers,janets@contoso.com,https://contoso.sharepoint.com/sites/Blog01
Contoso Blog Editors,opalca@contoso.com,https://contoso.sharepoint.com/sites/Blog01
Project Alpha Approvers,robinc@contoso.com,https://contoso.sharepoint.com/sites/Project01
```

For the next step, you must have the two CSV files saved to your drive. Here are example commands that use both CSV files and to add permissions and group membership:

```
Import-Csv C:\O365Admin\GroupsAndPermissions.csv | ForEach {New-SPOSiteGroup -Group $_.Group -
PermissionLevels $_.PermissionLevels -Site $_.Site}
Import-Csv C:\O365Admin\Users.csv | ForEach {Add-SPOUser -Group $_.Group -LoginName $_.LoginName -Site
$_.Site}
```

The script imports the CSV file contents and uses the values in the columns to populate the parameters of the **New-SPOSiteGroup** and **Add-SPOUser** commands. In our example, we're saving this file to the O365Admin folder on drive C, but you can save it wherever you want.

Now, let's remove a bunch of people for several groups in different sites using the same CSV file. Here's an example command:

```
Import-Csv C:\0365Admin\Users.csv | ForEach {Remove-SPOUser -LoginName $_.LoginName -Site $_.Site -Group $_.Group}
```

Generate user reports

You might want to get a report for a few sites and display the users for those sites, their permission level, and other properties. This is how the syntax looks:

```
$tenant = "<tenant name, such as litwareinc for litwareinc.com>"
$site = "<site name>"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | select * | Format-table -Wrap -AutoSize |
Out-File c:\UsersReport.txt -Force -Width 360 -Append
```

This will grab the data for these three sites and write them to a text file on your local drive. The parameter – Append will add new content to an existing file.

For example, let's run a report on the ContosoTest, TeamSite01, and Project01 sites for the Contoso1 tenant:

```
$tenant = "contoso"
$site = "contosotest"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | Format-Table -Wrap -AutoSize | Out-File
c:\UsersReport.txt -Force -Width 360 -Append
$site = "TeamSite01"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | Format-Table -Wrap -AutoSize | Out-File
c:\UsersReport.txt -Force -Width 360 -Append
$site = "Project01"
Get-SPOUser -Site https://$tenant.sharepoint.com/sites/$site | Format-Table -Wrap -AutoSize | Out-File
c:\UsersReport.txt -Force -Width 360 -Append
```

We had to change only the **\$site** variable. The **\$tenant** variable keeps its value through all three runs of the command.

However, what if you wanted to do this for every site? You can do this without having to type all those websites by using this command:

```
Get-SPOSite | ForEach {Get-SPOUser -Site $_.Url} | Format-Table -Wrap -AutoSize | Out-File
c:\UsersReport.txt -Force -Width 360 -Append
```

This report is fairly simple, and you can add more code to create more specific reports or reports that include more detailed information. But this should give you an idea of how to use the SharePoint Online Management Shell to manage users in the SharePoint Online environment.

See also

[Connect to SharePoint Online PowerShell](#)

[Manage SharePoint Online with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

Manage SharePoint Online site groups with PowerShell

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Although you can use the Microsoft 365 admin center, you can also use PowerShell for Microsoft 365 to manage your SharePoint Online site groups.

Before you begin

The procedures in this article require you to connect to SharePoint Online. For instructions, see [Connect to SharePoint Online PowerShell](#).

View SharePoint Online with PowerShell for Microsoft 365

The SharePoint Online admin center has some easy-to-use methods for managing site groups. For example, suppose you want to look at the groups, and the group members, for the

`https://litwareinc.sharepoint.com/sites/finance` site. Here's what you have to do to:

1. From the SharePoint admin center, select **Active sites**, and then select the URL of the site.
2. On the site page, select **Settings** (located in the upper right-hand corner of the page), and then select **Site permissions**.

And then repeat the process for the next site you want to look at.

To get a list of the groups with PowerShell for Microsoft 365, you can use the following commands:

```
$siteURL = "https://litwareinc.sharepoint.com/sites/finance"
$x = Get-SPOSiteGroup -Site $siteURL
foreach ($y in $x)
{
    Write-Host $y.Title -ForegroundColor "Yellow"
    Get-SPOSiteGroup -Site $siteURL -Group $y.Title | Select-Object -ExpandProperty Users
    Write-Host
}
```

There are two ways to run this command set in the SharePoint Online Management Shell command prompt:

- Copy the commands into Notepad (or another text editor), modify the value of the **\$siteURL** variable, select the commands, and then paste them into the SharePoint Online Management Shell command prompt. When you do, PowerShell will stop at a **> >** prompt. Press Enter to execute the `foreach` command.
- Copy the commands into Notepad (or another text editor), modify the value of the **\$siteURL** variable, and then save this text file with a name and the .ps1 extension in a suitable folder. Next, run the script from the SharePoint Online Management Shell command prompt by specifying its path and file name. Here is an example command:

```
C:\Scripts\SiteGroupsAndUsers.ps1
```

In both cases, you should see something similar to this:

```
Select Admin
PS C:\WINDOWS\system32> C:\scripts\SiteGroupsAndUsers.p
Excel Services Viewers
SHAREPOINT\system

Members
alex@litwareinc.com
allieb@litwareinc.com
annew@litwareinc.com
azizh@litwareinc.com
belindan@litwareinc.com
bonniek@litwareinc.com
robinc@litwareinc.com
davidl@litwareinc.com
zrinkam@litwareinc.com

Owners
doren@litwareinc.com
fabrice@litwareinc.com
garretv@litwareinc.com
garthf@litwareinc.com
janets@litwareinc.com
juliani@litwareinc.com
junminh@litwareinc.com
SHAREPOINT\system
tonyk@litwareinc.com
zrinkam@litwareinc.com

Visitors
mollyd@litwareinc.com
pavelb@litwareinc.com
sarad@litwareinc.com
```

These are all the groups that have been created for the site <https://litwareinc.sharepoint.com/sites/finance>, and all the users assigned to those groups. The group names are in yellow to help you separate group names from their members.

As another example, here is a command set that lists the groups, and all the group memberships, for all of your SharePoint Online sites.

```
$x = Get-SPOSite
foreach ($y in $x)
{
    Write-Host $y.Url -ForegroundColor "Yellow"
    $z = Get-SPOSiteGroup -Site $y.Url
    foreach ($a in $z)
    {
        $b = Get-SPOSiteGroup -Site $y.Url -Group $a.Title
        Write-Host $b.Title -ForegroundColor "Cyan"
        $b | Select-Object -ExpandProperty Users
        Write-Host
    }
}
```

See also

[Connect to SharePoint Online PowerShell](#)

[Create SharePoint Online sites and add users with PowerShell](#)

[Manage SharePoint Online users and groups with PowerShell](#)

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

How to use PowerShell to migrate email to Microsoft 365

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Administrators often migrate email from existing systems when they first set up Microsoft 365. The following articles describe how to migrate email by using Windows PowerShell:

- [Use PowerShell to perform a cutover migration to Microsoft 365](#)
- [Use PowerShell to perform an IMAP migration to Microsoft 365](#)
- [Use PowerShell to perform a staged migration to Microsoft 365](#)

Related topics

[Manage Microsoft 365 with PowerShell](#)

[Getting started with PowerShell for Microsoft 365](#)

[Manage SharePoint with PowerShell](#)

[Use Windows PowerShell to create reports in Microsoft 365](#)

[Why you need to use Microsoft 365 PowerShell](#)

[Manage Microsoft 365 user accounts, licenses, and groups with PowerShell](#)

Use PowerShell to perform a cutover migration to Microsoft 365

10/28/2022 • 9 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can migrate the contents of user mailboxes from a source email system to Microsoft 365 all at once by using a cutover migration. This article walks you through the tasks for an email cutover migration by using Exchange Online PowerShell.

By reviewing the topic, [What you need to know about a cutover email migration to Microsoft 365](#), you can get an overview of the migration process. When you're comfortable with the contents of that article, use this one to begin migrating mailboxes from one email system to another.

NOTE

You can also use the [Exchange admin center](#) to perform a cutover migration. See [Perform a cutover migration of email to Microsoft 365](#).

What do you need to know before you begin?

Estimated time to complete this task: 2-5 minutes to create a migration batch. After the migration batch is started, the duration of the migration will vary based on the number of mailboxes in the batch, the size of each mailbox, and your available network capacity. For information about other factors that affect how long it takes to migrate mailboxes to Microsoft 365, see [Migration Performance](#).

You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Migration" entry in a table in the [Recipients Permissions](#) topic.

To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

Migration steps

Step 1: Prepare for a cutover migration

- **Add your on-premises Exchange organization as an accepted domain of your Microsoft 365 organization.** The migration service uses the SMTP address of your on-premises mailboxes to create the Microsoft Online Services user ID and email address for the new Microsoft 365 mailboxes. Migration will fail if your Exchange domain isn't an accepted domain or the primary domain of your Microsoft 365 organization. For more information, see [Verify your domain](#).
- **Configure Outlook Anywhere on your on-premises Exchange server.** The email migration service uses RPC over HTTP, or Outlook Anywhere, to connect to your on-premises Exchange server. For information about how to set up Outlook Anywhere for Exchange 2010, Exchange 2007, and Exchange 2003, see the following:
 - [Exchange 2010: Enable Outlook Anywhere](#)

- [Exchange 2007: How to Enable Outlook Anywhere](#)
- [Exchange 2003: Deployment Scenarios for RPC over HTTP](#)
- [How to Configure Outlook Anywhere with Exchange 2003](#)

IMPORTANT

Your Outlook Anywhere configuration must be configured with a certificate issued by a trusted certification authority (CA). It can't be configured with a self-signed certificate. For more information, see [How to Configure SSL for Outlook Anywhere](#).

- **Verify that you can connect to your Exchange organization using Outlook Anywhere.** Try one of these methods to test your connection settings:
 - Use Microsoft Outlook from outside your corporate network to connect to your on-premises Exchange mailbox.
 - Use the Microsoft [Exchange Remote Connectivity Analyzer](#) to test your connection settings. Use the Outlook Anywhere (RPC over HTTP) or Outlook Autodiscover tests.
 - Run the following commands in Exchange Online PowerShell.

```
$Credentials = Get-Credential
```

```
Test-MigrationServerAvailability -ExchangeOutlookAnywhere -Autodiscover -EmailAddress <email address for on-premises administrator> -Credentials $credentials
```

- **Assign an on-premises user account the necessary permissions to access mailboxes in your Exchange organization.** The on-premises user account that you use to connect to your on-premises Exchange organization (also called the migration administrator) must have the necessary permissions to access the on-premises mailboxes that you want to migrate to Microsoft 365. This user account is used to create a migration endpoint to your on-premises organization.

The following list shows the administrative privileges required to migrate mailboxes using a cutover migration. There are three possible options.

- The migration administrator must be a member of the **Domain Admins** group in Active Directory in the on-premises organization.

Or

- The migration administrator must be assigned the **FullAccess** permission for each on-premises mailbox.

Or

- The migration administrator must be assigned the **Receive As** permission on the on-premises mailbox database that stores the user mailboxes.

- **Disable Unified Messaging.** If the on-premises mailboxes you're migrating are enabled for Unified Messaging (UM), you have to disable UM on the mailboxes before you migrate them. You can then enable UM on the mailboxes after the migration is complete.
- **Security Groups and Delegates** The email migration service cannot detect whether on-premises Active Directory groups are security groups or not, so it cannot provision any migrated groups as security groups in Microsoft 365. If you want to have security groups in your Microsoft 365 tenant, you

must first provision an empty mail-enabled security group in your Microsoft 365 tenant before starting the cutover migration. Additionally, this migration method only moves mailboxes, mail users, mail contacts, and mail-enabled groups. If any other Active Directory object, such as user that is not migrated to Microsoft 365, is assigned as a manager or delegate to an object being migrated, they must be removed from the object before you migrate.

Step 2: Create a migration endpoint

To migrate email successfully, Microsoft 365 needs to connect and communicate with the source email system. To do this, Microsoft 365 uses a migration endpoint. To create an Outlook Anywhere migration endpoint for cutover migration, first [connect to Exchange Online](#).

For a full list of migration commands, see [Move and migration cmdlets](#).

Run the following commands in Exchange Online PowerShell:

```
$Credentials = Get-Credential
```

The example uses the [Test-MigrationServerAvailability](#) cmdlet to obtain and test the connection settings to the on-premises Exchange server, and then uses those connection settings to create the migration endpoint called "CutoverEndpoint".

```
$TSMA = Test-MigrationServerAvailability -ExchangeOutlookAnywhere -Autodiscover -EmailAddress  
administrator@contoso.com -Credentials $credentials
```

```
New-MigrationEndpoint -ExchangeOutlookAnywhere -Name CutoverEndpoint -ConnectionSettings  
$TSMA.ConnectionSettings
```

NOTE

The **New-MigrationEndpoint** cmdlet can be used to specify a database for the service to use by using the -**TargetDatabase** option. Otherwise a database is randomly assigned from the Active Directory Federation Services (AD FS) 2.0 site where the management mailbox is located.

Verify it worked

In Exchange Online PowerShell, run the following command to display information about the "CutoverEndpoint" migration endpoint:

```
Get-MigrationEndpoint CutoverEndpoint | Format-List EndpointType,ExchangeServer,UseAutoDiscover,Max*
```

Step 3: Create the cutover migration batch

You can use the **New-MigrationBatch** cmdlet in Exchange Online PowerShell to create a migration batch for a cutover migration. You can create a migration batch and start it automatically by including the *AutoStart* parameter. Alternatively, you can create the migration batch and then manually start it afterwards by using the **Start-MigrationBatch** cmdlet. This example creates a migration batch called "CutoverBatch" and uses the migration endpoint that was created in the previous step.

```
New-MigrationBatch -Name CutoverBatch -SourceEndpoint CutoverEndpoint -AutoStart
```

This example also creates a migration batch called "CutoverBatch" and uses the migration endpoint that was

created in the previous step. Because the *AutoStart* parameter isn't included, the migration batch has to be manually started on the migration dashboard or by using **Start-MigrationBatch** cmdlet. As previously stated, only one cutover migration batch can exist at a time.

```
New-MigrationBatch -Name CutoverBatch -SourceEndpoint CutoverEndpoint
```

Verify it worked

To verify that you've successfully created a migration batch for a cutover migration, run the following command in Exchange Online PowerShell to display information about the new migration batch:

```
Get-MigrationBatch | Format-List
```

Step 4: Start the cutover migration batch

To start the migration batch in Exchange Online PowerShell, run the following command. This will create a migration batch called "CutoverBatch".

```
Start-MigrationBatch -Identity CutoverBatch
```

Verify it worked

If a migration batch is successfully started, its status on the migration dashboard is specified as Syncing. To verify that you've successfully started a migration batch using Exchange Online PowerShell, run the following command:

```
Get-MigrationBatch -Identity CutoverBatch | Format-List Status
```

Step 5: Route your email to Microsoft 365

Email systems use a DNS record called an MX record to figure out where to deliver emails. During the email migration process, your MX record was pointing to your source email system. Now that the email migration to Microsoft 365 is complete, it's time to point your MX record at Microsoft 365. This helps make sure that email is delivered to your Microsoft 365 mailboxes. By moving the MX record, you can also turn off your old email system when you're ready.

For many DNS providers, there are specific instructions to change your MX record. If your DNS provider isn't included, or if you want to get a sense of the general directions, [general MX record instructions](#) are provided as well.

It can take up to 72 hours for the email systems of your customers and partners to recognize the changed MX record. Wait at least 72 hours before you proceed to the next task: [Step 6: Delete the cutover migration batch](#).

Step 6: Delete the cutover migration batch

After you change the MX record and verify that all email is being routed to Microsoft 365 mailboxes, notify the users that their mail is going to Microsoft 365. After this, you can delete the cutover migration batch. Verify the following before you delete the migration batch.

- All users are using Microsoft 365 mailboxes. After the batch is deleted, mail sent to mailboxes on the on-premises Exchange Server isn't copied to the corresponding Microsoft 365 mailboxes.
- Microsoft 365 mailboxes were synchronized at least once after mail began being sent directly to them. To do this, make sure that the value in the Last Synced Time box for the migration batch is more recent than when mail started being routed directly to Microsoft 365 mailboxes.

To delete the "CutoverBatch" migration batch in Exchange Online PowerShell, run the following command:

Section 7: Assign user licenses

Activate Microsoft 365 user accounts for the migrated accounts by assigning licenses. If you don't assign a license, the mailbox is disabled when the grace period ends (30 days). To assign a license in the Microsoft 365 admin center, see [Assign or unassign licenses](#).

Step 8: Complete post-migration tasks

- **Create an Autodiscover DNS record so users can easily get to their mailboxes.** After all on-premises mailboxes are migrated to Microsoft 365, you can configure an Autodiscover DNS record for your Microsoft 365 organization to enable users to easily connect to their new Microsoft 365 mailboxes with Outlook and mobile clients. This new Autodiscover DNS record has to use the same namespace that you're using for your Microsoft 365 organization. For example, if your cloud-based namespace is cloud.contoso.com, the Autodiscover DNS record you need to create is autodiscover.cloud.contoso.com.

If you keep your Exchange Server, you should also make sure that Autodiscover DNS CNAME record has to point to Microsoft 365 in both internal and external DNS after the migration so that the Outlook client will to connect to the correct mailbox.

NOTE

In Exchange 2007, Exchange 2010, and Exchange 2013 you should also set

```
Set-ClientAccessServer AutodiscoverInternalConnectionURI to Null .
```

Microsoft 365 uses a CNAME record to implement the Autodiscover service for Outlook and mobile clients. The Autodiscover CNAME record must contain the following information:

- **Alias:** autodiscover
- **Target:** autodiscover.outlook.com

For more information, see [Add DNS records to connect your domain](#).

- **Decommission on-premises Exchange servers.** After you've verified that all email is being routed directly to the Microsoft 365 mailboxes, and you no longer need to maintain your on-premises email organization or don't plan on implementing a single sign-on (SSO) solution, you can uninstall Exchange from your servers and remove your on-premises Exchange organization.

For more information, see the following:

- [Modify or Remove Exchange 2010](#)
- [How to Remove an Exchange 2007 Organization](#)
- [How to Uninstall Exchange Server 2003](#)

Use PowerShell to perform an IMAP migration to Microsoft 365

10/28/2022 • 9 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

As part of the process of deploying Microsoft 365, you can choose to migrate the contents of user mailboxes from an Internet Mail Access Protocol (IMAP) email service to Microsoft 365. This article walks you through the tasks for an email IMAP migration by using Exchange Online PowerShell.

NOTE

You can also use the [Exchange admin center](#) to perform an IMAP migration. See [Migrate your IMAP mailboxes](#).

What do you need to know before you begin?

Estimated time to complete this task: 2-5 minutes to create a migration batch. After the migration batch is started, the duration of the migration will vary based on the number of mailboxes in the batch, the size of each mailbox, and your available network capacity. For information about other factors that affect how long it takes to migrate mailboxes to Microsoft 365, see [Migration Performance](#).

You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Migration" entry in a table in the [Recipients Permissions](#) topic.

To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

The following restrictions apply to IMAP migrations:

- Only items in a user's inbox or other mail folders can be migrated. You can't migrate contacts, calendar items, or tasks.
- A maximum of 500,000 items can be migrated from a user's mailbox.
- The maximum message size that can be migrated is 35 MB.

Migration steps

Step 1: Prepare for an IMAP migration

- **If you have a domain for your IMAP organization, add it as an accepted domain of your Microsoft 365 organization.** If you want to use the same domain you already own for your Microsoft 365 mailboxes, you first have to add it as an accepted domain to Microsoft 365. After you have added it, you can create your users in Microsoft 365. For more information, see [Verify your domain](#).
- **Add each user to Microsoft 365 so that they have a mailbox.** For instructions, see [Add users to Microsoft 365 for business](#).
- **Obtain the FQDN of the IMAP server.** You need to provide the fully qualified domain name (FQDN) (also called the full computer name) of the IMAP server that you will migrate mailbox data from when

you create an IMAP migration endpoint. Use an IMAP client or the PING command to verify that you can use the FQDN to communicate with the IMAP server over the Internet.

- **Configure the firewall to allow IMAP connections.** You might have to open ports in the firewall of the organization that hosts the IMAP server so network traffic originating from the Microsoft datacenter during the migration is allowed to enter the organization that hosts the IMAP server. For a list of IP addresses used by Microsoft datacenters, see [Exchange Online URLs and IP Address Ranges](#).
- **Assign the administrator account permissions to access mailboxes in your IMAP organization.** If you use administrator credentials in the CSV file, the account that you use must have the necessary permissions to access the on-premises mailboxes. The permissions required to access user mailboxes is determined by the particular IMAP server.
- **To use the Exchange Online PowerShell cmdlets,** you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

- **Verify that you can connect to your IMAP server.** Run the following command in Exchange Online PowerShell to test the connection settings to your IMAP server.

```
Test-MigrationServerAvailability -IMAP -RemoteServer <FQDN of IMAP server> -Port <143 or 993> -  
Security <None, Ssl, or Tls>
```

For the value of the **Port** parameter, it's typical to use 143 for unencrypted or Transport Layer Security (TLS) connections and to use 993 for SSL connections.

Step 2: Create a CSV file for an IMAP migration batch

Identify the group of users whose mailboxes you want to migrate in an IMAP migration batch. Each row in the CSV file contains information necessary to connect to a mailbox in the IMAP messaging system.

Here are the required attributes for each user:

- **EmailAddress** specifies the user ID for the user's Microsoft 365 mailbox.
- **UserName** specifies the logon name for the account to use to access the mailbox on the IMAP server.
- **Password** specifies the password for the account in the **UserName** column.

Here's an example of the format for the CSV file. In this example, three mailboxes are migrated:

```
EmailAddress,UserName>Password  
terrya@contoso.edu,terry.adams,1091990  
annb@contoso.edu,ann.beebe,2111991  
paulc@contoso.edu,paul.cannon,3281986
```

For the **UserName** attribute, in addition to the user name, you can use the credentials of an account that has been assigned the necessary permissions to access mailboxes on the IMAP server; the following are some of the specific formats used for some of the IMAP servers:

Microsoft Exchange:

If you're migrating email from the IMAP implementation for Microsoft Exchange, use the format **Domain/Admin_UserName/User_UserName** for the **UserName** attribute in the CSV file. Let's say you're migrating email from Exchange for Terry Adams, Ann Beebe, and Paul Cannon. You have a mail administrator account, where the user name is **mailadmin** and the password is **P@ssw0rd**. Here's what your CSV file would look like:

```
EmailAddress,UserName,Password
terrya@contoso.edu,contoso-students/mailadmin/terry.adams,P@ssw0rd
annb@contoso.edu,contoso-students/mailadmin/ann.beebe,P@ssw0rd
paulc@contoso.edu,contoso-students/mailadmin/paul.cannon,P@ssw0rd
```

Dovecot:

For IMAP servers that support Simple Authentication and Security Layer (SASL), such as a Dovecot IMAP server, use the format **User_UserName*Admin_UserName**, where the asterisk (*) is a configurable separator character. Let's say you're migrating those same users' email from a Dovecot IMAP server using the administrator credentials **mailadmin** and **P@ssw0rd**. Here's what your CSV file would look like:

```
EmailAddress,UserName,Password
terrya@contoso.edu,terry.adams*mailadmin,P@ssw0rd
annb@contoso.edu,ann.beebe*mailadmin,P@ssw0rd
paulc@contoso.edu,paul.cannon*mailadmin,P@ssw0rd
```

Mirapoint:

If you're migrating email from Mirapoint Message Server, use the format **#user@domain#Admin_UserName#** for the administrator credentials. To migrate email from Mirapoint using the administrator credentials **mailadmin** and **P@ssw0rd**, your CSV file would look like this:

```
EmailAddress,UserName,Password
terrya@contoso.edu,#terry.adams@contoso-students.edu#mailadmin#,P@ssw0rd
annb@contoso.edu,#ann.beebe@contoso-students.edu#mailadmin#,P@ssw0rd
paulc@contoso.edu,#paul.cannon@contoso-students.edu#mailadmin#,P@ssw0rd
```

Courier IMAP:

Some source email systems, such as Courier IMAP, don't support using mailbox admin credentials to migrate mailboxes to Microsoft 365. Instead, you can set up your source email system to use virtual shared folders. By using virtual shared folders, you can use the mailbox admin credentials to access user mailboxes on the source email system. For more information about how to configure virtual shared folders for Courier IMAP, see [Shared Folders](#).

To migrate mailboxes after you set up virtual shared folders on your source email system, you have to include the optional attribute **UserRoot** in the migration file. This attribute specifies the location of each user's mailbox in the virtual shared folder structure on the source email system. For example, the path to Terry's mailbox is `/users/terry.adams`.

Here's an example of a CSV file that contains the **UserRoot** attribute:

```
EmailAddress,UserName,Password,UserRoot
terrya@contoso.edu,mailadmin,P@ssw0rd,/users/terry.adams
annb@contoso.edu,mailadmin,P@ssw0rd,/users/ann.beebe
paulc@contoso.edu,mailadmin,P@ssw0rd,/users/paul.cannon
```

Step 3: Create an IMAP migration endpoint

To migrate email successfully, Microsoft 365 needs to connect to and communicate with the source email system. To do this, Microsoft 365 uses a migration endpoint. The migration endpoint also defines the number of mailboxes to migrate simultaneously and the number of mailboxes to synchronize simultaneously during incremental synchronization, which occurs once every 24 hours. To create a migration end point for IMAP migration, first [connect to Exchange Online](#).

For a full list of migration commands, see [Move and migration cmdlets](#).

To create the IMAP migration endpoint called "IMAPEndpoint" in Exchange Online PowerShell, run the following command:

```
New-MigrationEndpoint -IMAP -Name IMAPEndpoint -RemoteServer imap.contoso.com -Port 993 -Security Ssl
```

You can also add parameters to specify concurrent migrations, concurrent incremental migrations, and the port to use. The following Exchange Online PowerShell command creates an IMAP migration endpoint called "IMAPEndpoint" that supports 50 concurrent migrations and up to 25 concurrent incremental synchronizations. It also configures the endpoint to use port 143 for TLS encryption.

```
New-MigrationEndpoint -IMAP -Name IMAPEndpoint -RemoteServer imap.contoso.com -Port 143 -Security Tls -  
MaxConcurrentMigrations  
50 -MaxConcurrentIncrementalSyncs 25
```

For more information about the **New-MigrationEndpoint** cmdlet, see [New-MigrationEndpoint](#).

Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "IMAPEndpoint":

```
Get-MigrationEndpoint IMAPEndpoint | Format-List EndpointType,RemoteServer,Port,Security,Max*
```

Step 4: Create and start an IMAP migration batch

You can use the [New-MigrationBatch](#) cmdlet to create a migration batch for an IMAP migration. You can create a migration batch and start it automatically by including the *AutoStart* parameter. Alternatively, you can create the migration batch and then start it afterwards by using the [Start-MigrationBatch](#) cmdlet.

The following Exchange Online PowerShell command will automatically start the migration batch called "IMAPBatch1" using the IMAP endpoint called "IMAPEndpoint":

```
New-MigrationBatch -Name IMAPBatch1 -SourceEndpoint IMAPEndpoint -CSVData  
([System.IO.File]::ReadAllBytes("C:\Users\Administrator\Desktop\IMAPmigration_1.csv")) -AutoStart
```

Verify it worked

Run the [Get-MigrationBatch](#) cmdlet to display information about the "IMAPBatch1":

```
Get-MigrationBatch -Identity IMAPBatch1 | Format-List
```

You can also verify that the batch has started by running the following command:

```
Get-MigrationBatch -Identity IMAPBatch1 | Format-List Status
```

Step 5: Route your email to Microsoft 365

Email systems use a DNS record called an MX record to figure out where to deliver emails. During the email migration process, your MX record was pointing to your source email system. Now that the email migration to Microsoft 365 is complete, it's time to point your MX record at Microsoft 365. This helps make sure that email is delivered to your Microsoft 365 mailboxes. By moving the MX record, you can also turn off your old email system when you're ready.

For many DNS providers, there are specific instructions to change your MX record. If your DNS provider isn't

included, or if you want to get a sense of the general directions, [general MX record instructions](#) are provided as well.

It can take up to 72 hours for the email systems of your customers and partners to recognize the changed MX record. Wait at least 72 hours before you proceed to the next task: Step 6: Delete IMAP migration batch.

Step 6: Delete IMAP migration batch

After you change the MX record and verify that all email is being routed to Microsoft 365 mailboxes, notify the users that their mail is going to Microsoft 365. After this, you can delete the IMAP migration batch. Verify the following before you delete the migration batch.

- All users are using Microsoft 365 mailboxes. After the batch is deleted, mail sent to mailboxes on the on-premises Exchange Server isn't copied to the corresponding Microsoft 365 mailboxes.
- Microsoft 365 mailboxes were synchronized at least once after mail began being sent directly to them. To do this, make sure that the value in the Last Synced Time box for the migration batch is more recent than when mail started being routed directly to Microsoft 365 mailboxes.

To delete the "IMAPBatch1" migration batch from Exchange Online PowerShell, run the following command:

```
Remove-MigrationBatch -Identity IMAPBatch1
```

For more information about the **Remove-MigrationBatch** cmdlet, see [Remove-MigrationBatch](#).

Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "IMAPBatch1":

```
Get-MigrationBatch IMAPBatch1"
```

The command will return either the migration batch with a status of **Removing**, or it will return an error stating that migration batch couldn't be found, verifying that the batch was deleted.

For more information about the **Get-MigrationBatch** cmdlet, see [Get-MigrationBatch](#).

See also

[IMAP Migration Troubleshooter](#)

Use PowerShell to perform a staged migration to Microsoft 365

10/28/2022 • 11 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can migrate the contents of user mailboxes from a source email system to Microsoft 365 over time using a staged migration.

This article walks you through the tasks involved with for a staged email migration using Exchange Online PowerShell. The topic, [What you need to know about a staged email migration](#), gives you an overview of the migration process. When you're comfortable with the contents of that article, use this one to begin migrating mailboxes from one email system to another.

NOTE

You can also use the [Exchange admin center](#) to perform staged migration. See [Perform a staged migration of email to Microsoft 365](#).

What do you need to know before you begin?

Estimated time to complete this task: 2-5 minutes to create a migration batch. After the migration batch is started, the duration of the migration will vary based on the number of mailboxes in the batch, the size of each mailbox, and your available network capacity. For information about other factors that affect how long it takes to migrate mailboxes to Microsoft 365, see [Migration Performance](#).

You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Migration" entry in the [Recipients Permissions](#) topic.

To use the Exchange Online PowerShell cmdlets, you need to sign in and import the cmdlets into your local Windows PowerShell session. See [Connect to Exchange Online PowerShell](#) for instructions.

For a full list of migration commands, see [Move and migration cmdlets](#).

Migration steps

Step 1: Prepare for a staged migration

Before you migrate mailboxes to Microsoft 365 by using a staged migration, there are a few changes you must make to your Exchange environment.

Configure Outlook Anywhere on your on-premises Exchange Server The email migration service uses Outlook Anywhere (also known as RPC over HTTP), to connect to your on-premises Exchange Server. For information about how to set up Outlook Anywhere for Exchange Server 2007, and Exchange 2003, see the following:

- [Exchange 2007: How to Enable Outlook Anywhere](#)
- [How to configure Outlook Anywhere with Exchange 2003](#)

IMPORTANT

You must use a certificate issued by a trusted certification authority (CA) with your Outlook Anywhere configuration. Outlook Anywhere can't be configured with a self-signed certificate. For more information, see [How to configure SSL for Outlook Anywhere](#).

Optional: Verify that you can connect to your Exchange organization using Outlook Anywhere Try one of the following methods to test your connection settings.

- Use Outlook from outside your corporate network to connect to your on-premises Exchange mailbox.
- Use the [Microsoft Remote Connectivity Analyzer](#) to test your connection settings. Use the Outlook Anywhere (RPC over HTTP) or Outlook Autodiscover tests.
- Run the following commands in Exchange Online PowerShell:

```
$Credentials = Get-Credential
```

```
Test-MigrationServerAvailability -ExchangeOutlookAnywhere -Autodiscover -EmailAddress <email address  
for on-premises administrator> -Credentials $credentials
```

Set permissions The on-premises user account that you use to connect to your on-premises Exchange organization (also called the migration administrator) must have the necessary permissions to access the on-premises mailboxes that you want to migrate to Microsoft 365. This user account is used when you connect to your email system by creating a migration endpoint later in this procedure [Step 3: Create a migration endpoint](#).

To migrate the mailboxes, the admin must have one of the following permission sets:

- Be a member of the **Domain Admins** group in Active Directory in the on-premises organization.
- or
- Be assigned the **FullAccess** permission for each on-premises mailbox and the **WriteProperty** permission to modify the **TargetAddress** property on the on-premises user accounts.
- or
- Be assigned the **Receive As** permission on the on-premises mailbox database that stores user mailboxes and the **WriteProperty** permission to modify the **TargetAddress** property on the on-premises user accounts.

For instructions about how to set these permissions, see [Assign permissions to migrate mailboxes to Microsoft 365](#).

Disable Unified Messaging (UM) If UM is turned on for the on-premises mailboxes you're migrating, turn off UM before migration. Turn on UM for the mailboxes after migration is complete. For how-to steps, see [disable unified messaging](#).

Use directory synchronization to create new users in Microsoft 365. You use directory synchronization to create all the on-premises users in your Microsoft 365 organization.

You need to license the users after they're created. You have 30 days to add licenses after the users are created. For steps to add licenses, see [Step 8: Complete post-migration tasks](#).

You can use either the Microsoft Azure Active Directory (Azure AD) Synchronization Tool or the Microsoft Azure AD Sync Services to synchronize and create your on-premises users in Microsoft 365. After mailboxes are

migrated to Microsoft 365, you manage user accounts in your on-premises organization, and they're synchronized with your Microsoft 365 organization. For more information, see [Directory Integration](#).

Step 2: Create a CSV file for a staged migration batch

After you identify the users whose on-premises mailboxes you want to migrate to Microsoft 365, you use a comma separated value (CSV) file to create a migration batch. Each row in the CSV file—used by Microsoft 365 to run the migration—contains information about an on-premises mailbox.

NOTE

There isn't a limit for the number of mailboxes that you can migrate to Microsoft 365 using a staged migration. The CSV file for a migration batch can contain a maximum of 2,000 rows. To migrate more than 2,000 mailboxes, create additional CSV files and use each file to create a new migration batch.

Supported attributes

The CSV file for a staged migration supports the following three attributes. Each row in the CSV file corresponds to a mailbox and must contain a value for each of these attributes.

ATTRIBUTE	DESCRIPTION	REQUIRED?
EmailAddress	Specifies the primary SMTP email address, for example, pilarp@contoso.com, for on-premises mailboxes. Use the primary SMTP address for on-premises mailboxes and not user IDs from the Microsoft 365. For example, if the on-premises domain is named contoso.com but the Microsoft 365 email domain is named service.contoso.com, you would use the contoso.com domain name for email addresses in the CSV file.	Required
Password	The password to be set for the new Microsoft 365 mailbox. Any password restrictions that are applied to your Microsoft 365 organization also apply to the passwords included in the CSV file.	Optional
ForceChangePassword	Specifies whether a user must change the password the first time they sign in to their new Microsoft 365 mailbox. Use True or False for the value of this parameter. > [!NOTE]> If you've implemented a single sign-on (SSO) solution by deploying Active Directory Federation Services (AD FS) or greater in your on-premises organization, you must use False for the value of the ForceChangePassword attribute.	Optional

CSV file format

Here's an example of the format for the CSV file. In this example, three on-premises mailboxes are migrated to Microsoft 365.

The first row, or header row, of the CSV file lists the names of the attributes, or fields, specified in the rows that follow. Each attribute name is separated by a comma.

```
EmailAddress,Password,ForceChangePassword
pilarp@contoso.com,Pa$$w0rd,False
tobyn@contoso.com,Pa$$w0rd,False
briant@contoso.com,Pa$$w0rd,False
```

Each row under the header row represents one user and supplies the information that will be used to migrate the user's mailbox. The attribute values in each row must be in the same order as the attribute names in the header row.

Use any text editor, or an application like Excel , to create the CSV file. Save the file as a .csv or .txt file.

NOTE

If the CSV file contains non-ASCII or special characters, save the CSV file with UTF-8 or other Unicode encoding. Depending on the application, saving the CSV file with UTF-8 or other Unicode encoding can be easier when the system locale of the computer matches the language used in the CSV file.

Step 3: Create a migration endpoint

To migrate email successfully, Microsoft 365 needs to connect and communicate with the source email system. To do this, Microsoft 365 uses a migration endpoint. To create an Outlook Anywhere migration endpoint by using PowerShell, for staged migration, first [connect to Exchange Online](#).

For a full list of migration commands, see [Move and migration cmdlets](#).

To create an Outlook Anywhere migration endpoint called "StagedEndpoint" in Exchange Online PowerShell, run the following commands:

```
$Credentials = Get-Credential
```

```
New-MigrationEndpoint -ExchangeOutlookAnywhere -Name StagedEndpoint -Autodiscover -EmailAddress
administrator@contoso.com -Credentials $Credentials
```

For more information about the **New-MigrationEndpoint** cmdlet, see [New-MigrationEndpoint](#).

NOTE

The **New-MigrationEndpoint** cmdlet can be used to specify a database for the service to use by using the -**TargetDatabase** option. Otherwise a database is randomly assigned from the Active Directory Federation Services (AD FS) 2.0 site where the management mailbox is located.

Verify it worked

In Exchange Online PowerShell, run the following command to display information about the "StagedEndpoint" migration endpoint:

```
Get-MigrationEndpoint StagedEndpoint | Format-List EndpointType,ExchangeServer,UseAutoDiscover,Max*
```

Step 4: Create and start a stage migration batch

You can use the **New-MigrationBatch** cmdlet in Exchange Online PowerShell to create a migration batch for a cutover migration. You can create a migration batch and start it automatically by including the *AutoStart*

parameter. Alternatively, you can create the migration batch and then manually start it afterwards by using the **Start-MigrationBatch** cmdlet. This example creates a migration batch called "StagedBatch1" and uses the migration endpoint that was created in the previous step.

```
New-MigrationBatch -Name StagedBatch1 -SourceEndpoint StagedEndpoint -AutoStart
```

This example also creates a migration batch called "StagedBatch1" and uses the migration endpoint that was created in the previous step. Because the *AutoStart* parameter isn't included, the migration batch has to be manually started on the migration dashboard or by using **Start-MigrationBatch** cmdlet. As previously stated, only one cutover migration batch can exist at a time.

```
New-MigrationBatch -Name StagedBatch1 -SourceEndpoint StagedEndpoint
```

Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "StagedBatch1":

```
Get-MigrationBatch -Identity StagedBatch1 | Format-List
```

You can also verify that the batch has started by running the following command:

```
Get-MigrationBatch -Identity StagedBatch1 | Format-List Status
```

For more information about the **Get-MigrationBatch** cmdlet, see [Get-MigrationBatch](#).

Step 5: Convert on-premises mailboxes to mail-enabled users

After you have successfully migrated a batch of mailboxes, you need some way to let users get to their mail. A user whose mailbox has been migrated now has both a mailbox on-premises and one in Microsoft 365. Users who have a mailbox in Microsoft 365 will stop receiving new mail in their on-premises mailbox.

Because you are not done with your migrations, you are not yet ready to direct all users to Microsoft 365 for their email. So what do you do for those people who have both? What you can do is change the on-premises mailboxes that you've already migrated to mail-enabled users. When you change from a mailbox to a mail-enabled user, you can direct the user to Microsoft 365 for their email instead of going to their on-premises mailbox.

Another important reason to convert on-premises mailboxes to mail-enabled users is to retain proxy addresses from the Microsoft 365 mailboxes by copying proxy addresses to the mail-enabled users. This lets you manage cloud-based users from your on-premises organization by using Active Directory. Also, if you decide to decommission your on-premises Exchange Server organization after all mailboxes are migrated to Microsoft 365, the proxy addresses you've copied to the mail-enabled users will remain in your on-premises Active Directory.

Step 6: Delete a staged migration batch

After all mailboxes in a migration batch have been successfully migrated, and you've converted the on-premises mailboxes in the batch to mail-enabled users, you're ready to delete a staged migration batch. Be sure to verify that mail is being forwarded to the Microsoft 365 mailboxes in the migration batch. When you delete a staged migration batch, the migration service cleans up any records related to the migration batch and deletes the migration batch.

To delete the "StagedBatch1" migration batch in Exchange Online PowerShell, run the following command.

```
Remove-MigrationBatch -Identity StagedBatch1
```

For more information about the **Remove-MigrationBatch** cmdlet, see [Remove-MigrationBatch](#).

Verify it worked

Run the following command in Exchange Online PowerShell to display information about the "IMAPBatch1":

```
Get-MigrationBatch StagedBatch1
```

The command will return either the migration batch with a status of **Removing**, or it will return an error stating that migration batch couldn't be found, verifying that the batch was deleted.

For more information about the **Get-MigrationBatch** cmdlet, see [Get-MigrationBatch](#).

Step7: Assign licenses to Microsoft 365 users

Activate Microsoft 365 user accounts for the migrated accounts by assigning licenses. If you don't assign a license, the mailbox is disabled when the grace period (30 days) ends. To assign a license in the Microsoft 365 admin center, see [Assign or unassign licenses](#).

Step 8: Complete post-migration tasks

- **Create an Autodiscover DNS record so users can easily get to their mailboxes.** After all on-premises mailboxes are migrated to Microsoft 365, you can configure an Autodiscover DNS record for your Microsoft 365 organization to enable users to easily connect to their new Microsoft 365 mailboxes with Outlook and mobile clients. This new Autodiscover DNS record has to use the same namespace that you're using for your Microsoft 365 organization. For example, if your cloud-based namespace is cloud.contoso.com, the Autodiscover DNS record you need to create is autodiscover.cloud.contoso.com.

Microsoft 365 uses a CNAME record to implement the Autodiscover service for Outlook and mobile clients. The Autodiscover CNAME record must contain the following information:

- **Alias:** autodiscover
- **Target:** autodiscover.outlook.com

For more information, see [Add DNS records to connect your domain](#).

- **Decommission on-premises Exchange servers.** After you've verified that all email is being routed directly to the Microsoft 365 mailboxes, and you no longer need to maintain your on-premises email organization or don't plan on implementing an SSO solution, you can uninstall Exchange from your servers and remove your on-premises Exchange organization.

NOTE

Decommissioning Exchange can have unintended consequences. Before decommissioning your on-premises Exchange organization, we recommend that you contact Microsoft Support.

For more information, see the following:

- [Modify or Remove Exchange 2010](#)
- [How to Remove an Exchange 2007 Organization](#)
- [How to Uninstall Exchange Server 2003](#)

How to manage Microsoft 365 with Windows PowerShell for Delegated Access Permissions partners

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners. Many are network or telecom providers. They bundle Microsoft 365 subscriptions into their service offerings. When they sell a Microsoft 365 subscription, they're automatically granted Administer On Behalf Of (AOBO) permissions to the customer's tenancies so they can administer and report on those tenancies. These tasks are difficult to do in the Microsoft 365 admin center. It's much easier to use PowerShell for Microsoft 365 to do administrative tasks such as:

- List all the customer **TenantIds** and their domains
- Identify all users in a customer tenancy and their assigned licenses

NOTE

Some administrative tasks can only be done in PowerShell.

The following articles show how Syndication and CSP partners use PowerShell to administer their customer tenancies:

- [Manage Microsoft 365 tenants with Windows PowerShell for Delegated Access Permissions \(DAP\) partners](#)
- [Add a domain to a client tenancy with Windows PowerShell for Delegated Access Permission \(DAP\) partners](#)
- [Connect to Exchange Online PowerShell](#)
- [Retrieve customer tenant reporting data with Windows PowerShell for Delegated Access Permissions \(DAP\) partners](#)

Manage Microsoft 365 tenants with Windows PowerShell for Delegated Access Permissions (DAP) partners

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Windows PowerShell allows Syndication and Cloud Solution Provider (CSP) partners to easily administer and report on customer tenancy settings that are not available in the Microsoft 365 admin center. Note that Administer on Behalf Of (AOBO) permissions are required for the partner administrator account to connect to its customer tenancies.

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners. They are frequently network or telecom providers to other companies. They bundle Microsoft 365 subscriptions into their service offerings to their customers. When they sell a Microsoft 365 subscription, they are automatically granted Administer On Behalf Of (AOBO) permissions to the customer tenancies so they can administer and report on the customer tenancies.

What do you need to know before you begin?

The procedures in this topic require you to connect to [Connect to Microsoft 365 with PowerShell](#).

You also need your partner tenant administrator credentials.

What do you want to do?

List all tenant IDs

NOTE

If you have more than 500 tenants, scope the cmdlet syntax with either *-All* or *-MaxResultsParameter*. This applies to other cmdlets that can give a large output, such as **Get-MsolUser**.

To list all customer tenant IDs that you have access to, run this command.

```
Get-MsolPartnerContract -All | Select-Object TenantId
```

This will display a listing of all your customer tenants by **TenantId**.

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

Get a tenant ID by using the domain name

To get the **TenantId** for a specific customer tenant by domain name, run this command. Replace

<domainname.onmicrosoft.com> with the actual domain name of the customer tenant that you want.

```
Get-MsolPartnerContract -DomainName <domainname.onmicrosoft.com> | Select-Object TenantId
```

List all domains for a tenant

To get all domains for any one customer tenant, run this command. Replace *<customer TenantId value>* with the actual value.

```
Get-MsolDomain -TenantId <customer TenantId value>
```

If you have registered additional domains, this will return all domains associated with the customer **TenantId**.

Get a mapping of all tenants and registered domains

The previous PowerShell for Microsoft 365 commands showed you how to retrieve either tenant IDs or domains but not both at the same time, and with no clear mapping between them all. This command generates a listing of all your customer tenant IDs and their domains.

```
$Tenants = Get-MsolPartnerContract -All; $Tenants | foreach {$Domains = $_.TenantId; Get-MsolDomain -TenantId $Domains | fl @{Label="TenantId";Expression={$Domains}},name}
```

Get all users for a tenant

This will display the **UserPrincipalName**, the **DisplayName**, and the **isLicensed** status for all users for a particular tenant. Replace *<customer TenantId value>* with the actual value.

```
Get-MsolUser -TenantID <customer TenantId value>
```

Get all details about a user

If you want to see all the properties of a particular user, run this command. Replace *<customer TenantId value>* and *<user principal name value>* with the actual values.

```
Get-MsolUser -TenantId <customer TenantId value> -UserPrincipalName <user principal name value>
```

Add users, set options, and assign licenses

The bulk creation, configuration, and licensing of Microsoft 365 users is particularly efficient by using PowerShell for Microsoft 365. In this two-step process, you first create entries for all the users you want to add in a comma-separated value (CSV) file and then import that file by using PowerShell for Microsoft 365.

Create a CSV file

Create a CSV file by using this format:

```
UserPrincipalName,FirstName,LastName,DisplayName>Password,TenantId,UsageLocation,LicenseAssignment
```

where:

- **UsageLocation**: The value for this is the two-letter ISO country/region code of the user. The country/region codes can be looked up at the [ISO Online Browsing Platform](#). For example, the code for the United States is US, and the code for Brazil is BR.
- **LicenseAssignment**: The value for this uses this format: `syndication-account:<PROVISIONING_ID>`. For example, if you are assigning customer tenant users O365_Business_Premium licenses, the **LicenseAssignment** value looks like this: `syndication-account:O365_Business_Premium`. You will find the PROVISIONING_IDs in the Syndication Partner Portal that you have access to as a Syndication or CSP partner.

Import the CSV file and create the users

After you have your CSV file created, run this command to create user accounts with non-expiring passwords that the user must change at first sign-in and that assigns the license you specify. Be sure to substitute the correct CSV file name.

```
Import-Csv .\FILENAME.CSV | foreach {New-MsolUser -UserPrincipalName $_.UserPrincipalName -DisplayName $_.DisplayName -FirstName $_.FirstName -LastName $_.LastName -Password $_.Password -UsageLocation $_.UsageLocation -LicenseAssignment $_.LicenseAssignment -ForceChangePassword:$true -PasswordNeverExpires:$true -TenantId $_.TenantId}
```

See also

[Help for partners](#)

Add a domain to a client tenancy with Windows PowerShell for Delegated Access Permission (DAP) partners

10/28/2022 • 3 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

You can create and associate new domains with your customer's tenancy with PowerShell for Microsoft 365 faster than using the Microsoft 365 admin center.

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners. They are frequently network or telecom providers to other companies. They bundle Microsoft 365 subscriptions into their service offerings to their customers. When they sell a Microsoft 365 subscription, they are automatically granted Administer On Behalf Of (AOBO) permissions to the customer tenancies so they can administer and report on the customer tenancies.

What do you need to know before you begin?

The procedures in this topic require you to connect to [Connect to Microsoft 365 with PowerShell](#).

You also need your partner tenant administrator credentials.

You also need the following information:

- You need the fully qualified domain name (FQDN) that your customer wants.
- You need the customer's **TenantId**.
- The FQDN must be registered with an Internet domain name service (DNS) registrar, such as GoDaddy. For more information on how to publically register a domain name, see [How to buy a domain name](#).
- You need to know how to add a TXT record to the registered DNS zone for your DNS registrar. For more information on how to add a TXT record, see [Add DNS records to connect your domain](#). If those procedures don't work for you, you will need to find the procedures for your DNS registrar.

Create domains

Your customers will likely ask you to create additional domains to associate with their tenancy because they don't want the default <domain>.onmicrosoft.com domain to be the primary one that represents their corporate identities to the world. This procedure walks you through creating a new domain associated with your customer's tenancy.

NOTE

To perform some of these operations, the partner administrator account you sign in with must be set to **Full administration** for the **Assign administrative access to companies you support** setting found in the details of the admin account in the [Microsoft 365 admin center](#). For more information on managing partner administrator roles, see [Partners: Offer delegated administration](#).

Create the domain in Azure Active Directory

This command creates the domain in Azure Active Directory but does not associate it with the publicly

registered domain. That comes when you prove that you own the publicly registered domain to Microsoft Microsoft 365 for enterprises.

```
New-MsolDomain -TenantId <customer TenantId> -Name <FQDN of new domain>
```

NOTE

PowerShell Core does not support the Microsoft Azure Active Directory Module for Windows PowerShell module and cmdlets with **Msol** in their name. To continue using these cmdlets, you must run them from Windows PowerShell.

Get the data for the DNS TXT verification record

Microsoft 365 will generate the specific data that you need to place into the DNS TXT verification record. To get the data, run this command.

```
Get-MsolDomainVerificationDNS -TenantId <customer TenantId> -DomainName <FQDN of new domain> -Mode  
DnsTxtRecord
```

This will give you output like:

```
Label: domainname.com
```

```
Text: MS=ms#####
```

```
Ttl: 3600
```

NOTE

You will need this text to create the TXT record in the publicly registered DNS zone. Be sure to copy and save it.

Add a TXT record to the publicly registered DNS zone

Before Microsoft 365 will start accepting traffic that is directed to the publicly registered domain name, you must prove that you own and have administrator permissions to the domain. You prove you own the domain by creating a TXT record in the domain. A TXT record doesn't do anything in your domain, and it can be deleted after your ownership of the domain is established. To create the TXT records, follow the procedures at [Add DNS records to connect your domain](#). If those procedures don't work for you, you need to find the procedures for your DNS registrar.

Confirm the successful creation of the TXT record via nslookup. Follow this syntax.

```
nslookup -type=TXT <FQDN of registered domain>
```

This will give you output like:

```
Non-authoritative answer:
```

```
FQDN of the registered domain
```

```
text=MS=ms#####
```

Validate domain ownership in Microsoft 365

In this last step, you validate to Microsoft 365 that you own the publicly registered domain. After this step, Microsoft 365 will begin accepting traffic routed to the new domain name. To complete the domain creation and registration process, run this command.

```
Confirm-MsolDomain -TenantId <customer TenantId> -DomainName <FQDN of new domain>
```

This command won't return any output, so to confirm that this worked, run this command.

```
Get-MsolDomain -TenantId <customer TenantId> -DomainName <FQDN of new domain>
```

This will return something like this

Name	Status	Authentication
-----	-----	-----
FQDN of new domain	Verified	Managed

See also

[Help for partners](#)

Retrieve customer tenant reporting data with Windows PowerShell for Delegated Access Permissions (DAP) partners

10/28/2022 • 2 minutes to read • [Edit Online](#)

This article applies to both Microsoft 365 Enterprise and Office 365 Enterprise.

Use remote Windows PowerShell for Microsoft Exchange Online to retrieve reports from individual customer tenants.

Syndication and Cloud Solution Provider (CSP) partners can access the data that makes up customer tenant reports directly via remote Windows PowerShell for Exchange Online PowerShell. This method lets partners collect and save the reporting data and then perform other operations on it. After you open a remote connection, retrieving reporting data about a customer tenancy is identical to running any cmdlet against a customer tenancy.

This article describes how you can use remote Windows PowerShell for Exchange Online to connect to a single customer tenancy and retrieve a report. By default, Windows PowerShell does not support aggregating reporting data from multiple customer tenancies. The reports you retrieve with this procedure are only for the *DelegatedOrg* that you connect to.

Before you begin

- Connect to your Exchange Online tenant by using remote Windows PowerShell. For instructions, see [Connect to Exchange Online tenants with remote Windows PowerShell for Delegated Access Permissions \(DAP\) partners](#)

Run the Get-StaleMailboxReport sample

After you have opened a remote session to Exchange Online, run the following command to retrieve the **Get-StaleMailboxReport** for the date range 03/25/2015 through 03/31/2015.

```
Get-StaleMailboxReport -StartDate 03/25/2015 -EndDate 03/31/2015
```

There are many other reporting cmdlets available for Exchange Online, Lync Online, SharePoint Online, and other services for message tracing that you can use. To learn more about the available reporting cmdlets, see the articles listed in the following section.

See also

[Office 365 Reporting web service](#)

[Reporting cmdlets in Exchange Online](#)

[Help for partners](#)

Use the Centralized Deployment PowerShell cmdlets to manage add-ins

10/28/2022 • 4 minutes to read • [Edit Online](#)

As a Microsoft 365 global admin, you can deploy Office Add-ins to users via the Centralized Deployment feature (see [Deploy Office Add-ins in the admin center](#)). In addition to deploying Office Add-ins via the Microsoft 365 admin center, you can also use Microsoft PowerShell. Install the [O365 Centralized Add-In Deployment Module for Windows PowerShell](#).

After you download the module, open a regular Windows PowerShell window and run the following cmdlet:

```
Import-Module -Name O365CentralizedAddInDeployment
```

Connect using your admin credentials

Before you can use the Centralized Deployment cmdlets, you need to sign in.

1. Start PowerShell.
2. Connect to PowerShell by using your company admin credentials. Run the following cmdlet.

```
Connect-OrganizationAddInService
```

3. In the **Enter Credentials** page, enter your Microsoft 365 **User Admin**, or **Global admin** credentials. Alternately, you can enter your credentials directly into the cmdlet.

Run the following cmdlet specifying your company admin credentials as a `PSCredential` object.

```
$secpasswd = ConvertTo-SecureString "MyPassword" -AsPlainText -Force
$mycredentials = New-Object System.Management.Automation.PSCredential ("serviceaccount@contoso.com",
$secpasswd)
Connect-OrganizationAddInService -Credential $mycredentials
```

NOTE

For more information about using PowerShell, see [Connect to Microsoft 365 with PowerShell](#).

Upload an add-in manifest

Run the **New-OrganizationAdd-In** cmdlet to upload an add-in manifest from a path, which can be either a file location or URL. The following example shows a file location for the value of the *ManifestPath* parameter.

```
New-OrganizationAddIn -ManifestPath 'C:\Users\Me\Desktop\taskpane.xml' -Locale 'en-US'
```

You can also run the **New-OrganizationAdd-In** cmdlet to upload an add-in and assign it to users or groups directly by using the *Members* parameter, as shown in the following example. Separate the email addresses of members with a comma.

```
New-OrganizationAddIn -ManifestPath 'C:\Users\Me\Desktop\taskpane.xml' -Locale 'en-US' -Members  
'KathyBonner@contoso.com', 'MaxHargrave@contoso.com'
```

Upload an add-in from the Office Store

Run the **New-OrganizationAddIn** cmdlet to upload a manifest from the Office Store.

In the following example, the **New-OrganizationAddIn** cmdlet specifies the *AssetId* for an add-in for a United States location and content market.

```
New-OrganizationAddIn -AssetId 'WA104099688' -Locale 'en-US' -ContentMarket 'en-US'
```

To determine the value for the *AssetId* parameter, you can copy it from the URL of the Office Store webpage for the add-in. AssetIds always begin with "WA" followed by a number. For example, in the previous example, the source for the *AssetId* value of WA104099688 is the Office Store webpage URL for the add-in:

<https://store.office.com/en-001/app.aspx?assetid=WA104099688>.

The values for the *Locale* parameter and the *ContentMarket* parameter are identical and indicate the country/region you're trying to install the add-in from. The format is en-US, fr-FR. and so forth.

NOTE

Add-ins uploaded from the Office Store will update automatically within a few days of the latest update being available on the Office Store.

Get details of an add-in

Run the **Get-OrganizationAddIn** cmdlet as shown below to get details of all add-ins uploaded to the tenant, including an add-in's product ID.

```
Get-OrganizationAddIn
```

Run the **Get-OrganizationAddIn** cmdlet with a value for the *ProductId* parameter to specify which add-in you want to retrieve details for.

```
Get-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122
```

To get full details of all the add-ins plus the assigned users and groups, pipe the output of the **Get-OrganizationAddIn** cmdlet to the **Format-List** cmdlet, as shown in the following example.

```
foreach($G in (Get-organizationAddIn)){Get-OrganizationAddIn -ProductId $G.ProductId | Format-List}
```

Turn on or turn off an add-in

To turn off an add-in so users and groups that are assigned to it will no longer have access, run the **Set-OrganizationAddIn** cmdlet with the *ProductId* parameter and the *Enabled* parameter set to `$false`, as shown in the following example.

```
Set-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -Enabled $false
```

To turn an add-in back on, run the same cmdlet with the *Enabled* parameter set to `$true`.

```
Set-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -Enabled $true
```

Add or remove users from an add-in

To add users and groups to a specific add-in, run the **Set-OrganizationAddInAssignments** cmdlet with the *ProductId*, *Add*, and *Members* parameters. Separate the email addresses of members with a comma.

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -Add -Members  
'KathyBonner@contoso.com','sales@contoso.com'
```

To remove users and groups, run the same cmdlet using the *Remove* parameter.

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -Remove -Members  
'KathyBonner@contoso.com','sales@contoso.com'
```

To assign an add-in to all users on the tenant, run the same cmdlet using the *AssignToEveryone* parameter with the value set to `$true`.

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -AssignToEveryone $true
```

To not assign an add-in to everyone and revert to the previously assigned users and groups, you can run the same cmdlet and turn off the *AssignToEveryone* parameter by setting its value to `$false`.

```
Set-OrganizationAddInAssignments -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -AssignToEveryone $false
```

Update an add-in

To update an add-in from a manifest, run the **Set-OrganizationAddIn** cmdlet with the *ProductId*, *ManifestPath*, and *Locale* parameters, as shown in the following example.

```
Set-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122 -ManifestPath  
'C:\Users\Me\Desktop\taskpane.xml' -Locale 'en-US'
```

NOTE

Add-ins uploaded from the Office Store will update automatically within a few days of the latest update being available on the Office Store.

Delete an add-in

To delete an add-in, run the **Remove-OrganizationAddIn** cmdlet with the *ProductId* parameter, as shown in the following example.

```
Remove-OrganizationAddIn -ProductId 6a75788e-1c6b-4e9b-b5db-5975a2072122
```


Get detailed help for each cmdlet

You can look at detailed help for each cmdlet by using the Get-help cmdlet. For example, the following cmdlet provides detailed information about the Remove-OrganizationAddIn cmdlet.

```
Get-help Remove-OrganizationAddIn -Full
```

Windows and Office 365 deployment lab kit

10/28/2022 • 2 minutes to read • [Edit Online](#)

The Windows and Office 365 deployment lab kit is designed to help you plan, test, and validate your deployment and management of desktops running Windows 10 Enterprise or Windows 11 Enterprise and Microsoft 365 Apps for enterprise. The labs in the kit cover using Microsoft Endpoint Configuration Manager, OneDrive, Windows Autopilot, and more. This kit is highly recommended for organizations preparing for desktop upgrades. As an isolated environment, the lab is also ideal for exploring deployment tool updates and testing your deployment-related automation.

There are two versions of the lab available for free download:

WINDOWS 10 LAB	WINDOWS 11 LAB
Windows 10 lab environment	Windows 11 lab environment
Windows 10 lab guides	Windows 11 lab guides

A complete lab environment

The lab provides you with an automatically provisioned virtual lab environment, including domain-joined desktop clients, a domain controller, an internet gateway, and a fully configured Configuration Manager instance. The labs include evaluation versions of the following products:

WINDOWS 10 LAB	WINDOWS 11 LAB
Windows 10 Enterprise, Version 21H2	Windows 11 Enterprise
Microsoft Endpoint Configuration Manager, Version 2103	Microsoft Endpoint Configuration Manager, Version 2203
Windows Assessment and Deployment Kit for Windows 10	Windows Assessment and Deployment Kit for Windows 11
Windows Server 2019	Windows Server 2022

The labs are also designed to be connected to trials for:

- Microsoft 365 E5
- Microsoft 365 Apps for enterprise
- Office 365 E5 with Enterprise Mobility + Security (EMS)

Step-by-step labs

Detailed lab guides take you through multiple deployment and management scenarios. The labs have been updated for the latest versions of Intune and Configuration Manager. Note: A new Windows 11 version of the lab is now available. The lab guides include the following scenarios:

Plan and prepare infrastructure

- Cloud Management Gateway
- Tenant attach and co-management
- Endpoint analytics

- Optimize update delivery

Deploy Windows

- OS deployment task sequences in Configuration Manager
- Windows Autopilot

Service Windows

- Servicing Windows using Group Policy
- Servicing Windows using Microsoft Intune
- Servicing Windows with Configuration Manager

Deploy Microsoft 365 Apps for enterprise

- Cloud managed deployment
- Locally managed deployment
- Microsoft 365 Apps for enterprise Deployment on Non-AD Joined Devices
- Enterprise managed deployment using Configuration Manager
- Enterprise managed deployment using Microsoft Intune
- Servicing Microsoft 365 Apps for enterprise using Configuration Manager
- Servicing Microsoft 365 Apps for enterprise using Intune
- LOB Deployment and Management with Microsoft Intune
- Deploy Microsoft Teams
- Assignment filters

Managing Microsoft Edge

- Deploy and Update Edge
- IE Mode
- Setup Enterprise New Tab Page

Security and Compliance

- BitLocker
- Microsoft Defender Antivirus
- Windows Hello for Business
- Windows Defender Credential Guard
- Microsoft Defender Application Guard
- Windows Defender Exploit Guard
- Windows Defender Application Control
- Microsoft Defender for Endpoint

NOTE

Please use a broadband internet connection to download this content and allow approximately 30 minutes for automatic provisioning. The lab environment requires a minimum of 16 GB of available memory and 150 GB of free disk space. For optimal performance, 32 GB of available memory and 300 GB of free space is recommended. The Windows client virtual machines expire 90 days after activation of the lab. New versions of the labs will be published on or before November 5, 2022.

Additional guidance

- [Windows client deployment resources and documentation](#)
- [Desktop Deployment series videos from Microsoft Mechanics](#)

- [Microsoft Endpoint Configuration Manager OS Deployment](#)
- [Deployment guide for Microsoft 365 Apps](#)
- [Getting Started with Intune](#)

Related resources

- [Introducing Microsoft 365](#)
- [Microsoft 365 for business](#)
- [Introducing Enterprise Mobility + Security](#)
- [Windows for business](#)

Microsoft 365 for enterprise Test Lab Guides

10/28/2022 • 2 minutes to read • [Edit Online](#)

This applies to both Microsoft 365 for enterprise and Office 365 Enterprise.

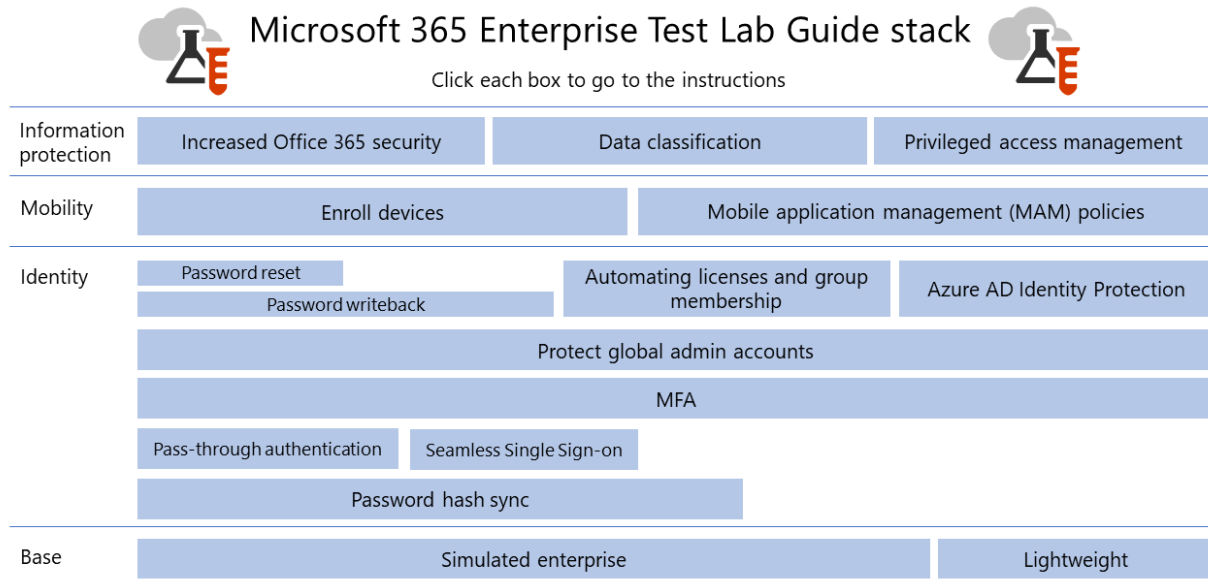
Test Lab Guides (TLGs) help you quickly learn about Microsoft products. They provide prescriptive instructions to configure simplified but representative test environments. You can use these environments for demonstration, customization, or creation of complex proofs of concept for the duration of a trial or paid subscription.

TLGs are designed to be modular. They build upon each other to create multiple configurations that more closely match your learning or test configuration needs. The "I built it out myself and it works" hands-on experience helps you understand the deployment requirements of a new product or scenario, so that you can better plan for hosting it in production.

You can also use TLGs to create representative environments to develop and test applications, also known as dev/test environments.



For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, expand the following graphic or go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).



<http://aka.ms/m365etlgs>

Start at the bottom of the stack and work your way up.

As of: 11/4/2019

Base configuration

First, create a test environment for [Microsoft 365 for enterprise](#). You can create two different types of base configurations:

- [Lightweight base configuration](#) - Use this when you want to configure and demonstrate Microsoft 365 for enterprise features and capabilities in a cloud-only environment, which does not include any on-premises components.

- [Simulated enterprise base configuration](#) - Use this when you want to configure and demonstrate Microsoft 365 for enterprise features and capabilities in a hybrid cloud environment, which uses on-premises components such as an Active Directory Domain Services (AD DS) domain.

You can also create test environments for Office 365 E5 by not adding the Microsoft 365 E5 license to your trial or production test environment.

Identity

To demonstrate identity-related features and capabilities, see:

- [Password hash synchronization](#)
Enable and test password hash-based directory synchronization from an AD DS domain controller.
- [Pass-through authentication](#)
Enable and test pass-through authentication to an AD DS domain controller.
- [Federated authentication](#)
Enable and test federated authentication to an AD DS domain controller.
- [Azure AD Seamless Single Sign-on](#)
Enable and test Azure AD Seamless Single Sign-on (Seamless SSO) with an AD DS domain controller.
- [Multi-factor authentication](#)
Enable and test smart phone-based multi-factor authentication for a specific user account.
- [Protect global administrator accounts](#)
Lock down your global administrator accounts with conditional access policies.
- [Password writeback](#)
Use password writeback to change the password on your AD DS user account from Azure AD.
- [Password reset](#)
Use self-service password reset to reset your password.
- [Automatic licensing and group membership](#)
Make administering new accounts easier than ever with automatic licensing and dynamic group membership.
- [Azure AD Identity Protection](#)
Scan your current user accounts for vulnerabilities.
- [Identity and device access](#)
Create an environment to test recommended identity and device access configurations and conditional access policies.

Mobile device management

To demonstrate mobile device management-related features and capabilities, see:

- [Device compliance policies](#)

Create a user group and a device compliance policy for Windows 10 devices.

- [Enroll iOS and Android devices](#)

Enroll iOS or Android devices and manage them remotely.

Information protection

To demonstrate information protection-related features and capabilities, see:

- [Increased Microsoft 365 security](#)

Configure settings for increased Microsoft 365 security and investigate built-in security tools.

- [Data classification](#)

Configure and apply labels to a document in a SharePoint Online team site.

- [Privileged access management](#)

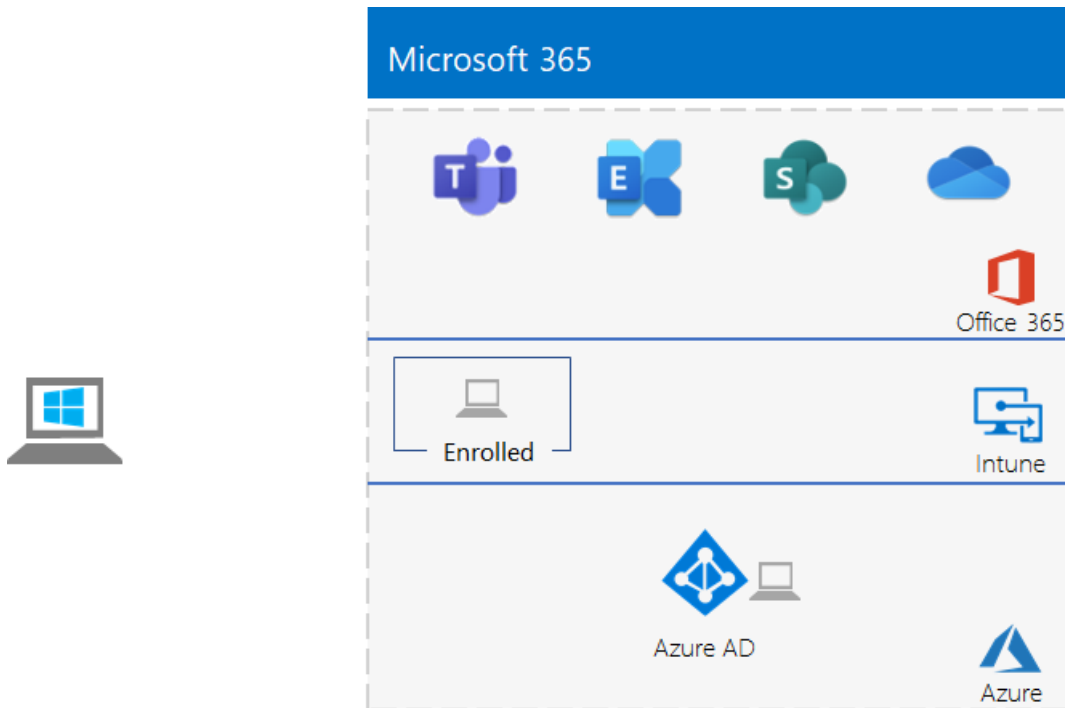
Configure privileged access management for just-in-time access to elevated and privileged tasks in your organization.

The lightweight base configuration

10/28/2022 • 10 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

This article describes how to create a simplified environment with a Microsoft 365 E5 subscription and a computer running Windows 10 Enterprise.



Creating a lightweight test environment involves five phases:

- [Phase 1: Create your Microsoft 365 E5 subscription](#)
- [Phase 2: Configure your Office 365 trial subscription](#)
- [Phase 3: Add a Microsoft 365 E5 trial subscription](#)
- [Phase 4: Create a Windows 10 Enterprise computer](#)
- [Phase 5: Join your Windows 10 computer to Azure AD](#)

Use the resulting environment to test the features and functionality of [Microsoft 365 for enterprise](#).



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, see [Microsoft 365 for enterprise Test Lab Guide Stack](#).

NOTE

You might want to print this article to record the specific information that you will need for this environment over the 30 days of the Office 365 trial subscription. You can easily extend the trial subscription for another 30 days. For a permanent test environment, create a new paid subscription with a separate Azure AD tenant and a small number of licenses.

Phase 1: Create your Microsoft 365 E5 subscription

We start with an Microsoft 365 E5 trial subscription and then add the Microsoft 365 E5 subscription to it.

NOTE

We recommend that you create a trial subscription of Office 365 so that your test environment has a separate Azure AD tenant from any paid subscriptions you currently have. This separation means that you can add and remove users and groups in the test tenant without affecting your production subscriptions.

To start your Microsoft 365 E5 trial subscription, you first need a fictitious company name and a new Microsoft account.

1. We recommend that you use a variant of the company name Contoso for your company name, which is a fictitious company used in Microsoft sample content, but it isn't required. Record your fictitious company name here: _____
2. To sign up for a new Microsoft account, go to <https://outlook.com> and create an account with a new email account and address. You will use this account to sign up for Office 365.
 - Record the first and last name of your new account here: _____
 - Record the new email account address here: _____@outlook.com

Sign up for an Office 365 E5 trial subscription

1. In your browser, go to <https://aka.ms/e5trial>.
2. In step 1 of the **Thank you for choosing Office 365 E5** page, enter your new email account address.
3. In step 2 of the trial subscription process, enter the requested information, and then perform the verification.
4. In step 3, enter an organization name and then an account name that will be the global admin for the subscription.
5. For step 4, record the sign-in page here (select and copy): _____
6. Record the user ID here: _____onmicrosoft.com
Record the password that you entered in a secure location. This value will be referred to as the **global administrator name**.
7. Select **Go to Setup**.
8. In Office 365 E5 Setup, select **Continue using *your organization*.onmicrosoft.com for email and signing in**, and then select **Exit and continue later**.

You should see the Microsoft 365 admin center.

Phase 2: Configure your Office 365 trial subscription

In this phase, you configure your subscription with additional users and assign them Office 365 E5 licenses.

To connect to your subscription with the Azure Active Directory PowerShell for Graph module from your computer, use the instructions in [Connect to Microsoft 365 with PowerShell](#).

In the **Windows PowerShell Credential Request** dialog box, enter the global administrator name (for example, *jdoe@contosotoycompany.onmicrosoft.com*) and password.

Fill in your organization name (for example, *contosotoycompany*), the two-character country code for your location, a common account password, and then run the following commands from the PowerShell prompt:

```
$orgName="<organization name>"
$loc="<two-character country code, such as US>"
$commonPW="<common user account password>"
$PasswordProfile=New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
$PasswordProfile.Password=$commonPW

$License = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicense
$License.SkuId = (Get-AzureADSubscribedSku | Where-Object -Property SkuPartNumber -Value "ENTERPRISEPREMIUM" -EQ).SkuId
$LicensesToAssign = New-Object -TypeName Microsoft.Open.AzureAD.Model.AssignedLicenses
$LicensesToAssign.AddLicenses = $License

for($i=2;$i -le 4; $i++) {
    $userUPN= "user${$i}@${$orgName}.onmicrosoft.com"
    New-AzureADUser -DisplayName "User ${$i}" -GivenName User -SurName $i -UserPrincipalName $userUPN -
UsageLocation $loc -AccountEnabled $true -PasswordProfile $PasswordProfile -MailNickName "user${$i}"
    $userObjectID = (Get-AzureADUser -SearchString $userupn).ObjectID
    Set-AzureADUserLicense -ObjectID $userObjectID -AssignedLicenses $LicensesToAssign
}
```

NOTE

The use of a common password here is for automation and ease of configuration for a test environment. Obviously, this is highly discouraged for production subscriptions.

Record key information for future reference

If you haven't already recorded these values, record them now:

- Global administrator name: _____onmicrosoft.com (from step 6 of Phase 1)

Also record the password for this account in a secure location.

- Your trial subscription organization name: _____ (from step 4 of Phase 1)
- To list the accounts for User 2, User 3, User 4, and User 5, run the following command from the Windows Azure Active Directory Module for Windows PowerShell prompt:

```
Get-AzureADUser | Sort UserPrincipalName | Select UserPrincipalName
```

Record the account names here:

- User 2 account name: user2@_____onmicrosoft.com
- User 3 account name: user3@_____onmicrosoft.com
- User 4 account name: user4@_____onmicrosoft.com
- User 5 account name: user5@_____onmicrosoft.com

Also record the common password for these accounts in a secure location.

Using an Office 365 test environment

If you need only an Office 365 test environment, you do not need to read the rest of this article.

For additional Test Lab Guides that apply to both Office 365 and Microsoft 365, see [Microsoft 365 for enterprise Test Lab Guides](#).

Phase 3: Add a Microsoft 365 E5 trial subscription

In this phase, you sign up for the Microsoft 365 E5 trial subscription and add it to the same organization as your Office 365 E5 trial subscription.

First, add the Microsoft 365 E5 trial subscription and assign the new Microsoft 365 license to your global administrator account.

1. In an internet browser private window, use your global administrator account credentials to sign in to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. On the **Microsoft 365 admin center** page, in the left navigation, select **Billing** > [Purchase services](#).
3. On the **Purchase services** page, select **Microsoft 365 E5**, and then select **Get free trial**.
4. On the **Microsoft 365 E5 Trial** page, decide to receive a text message or a phone call, enter your phone number, and then select **Text me** or **Call me**. Perform the verification.
5. On the **Confirm your order** page, select **Try now**.
6. On the **Order receipt** page, select **Continue**.
7. In the Microsoft 365 admin center, select **Users** > [Active users](#).
8. In **Active users**, select your administrator account.
9. Select **Licenses and apps**.
10. Disable the license for Office 365 Enterprise E5 and enable the license for Microsoft 365 E5.
11. Select **Save changes**, and then close the user account information pane.

Next, repeat steps 8 through 11 of the previous procedure for all of your other accounts (User 2, User 3, User 4, and User 5).

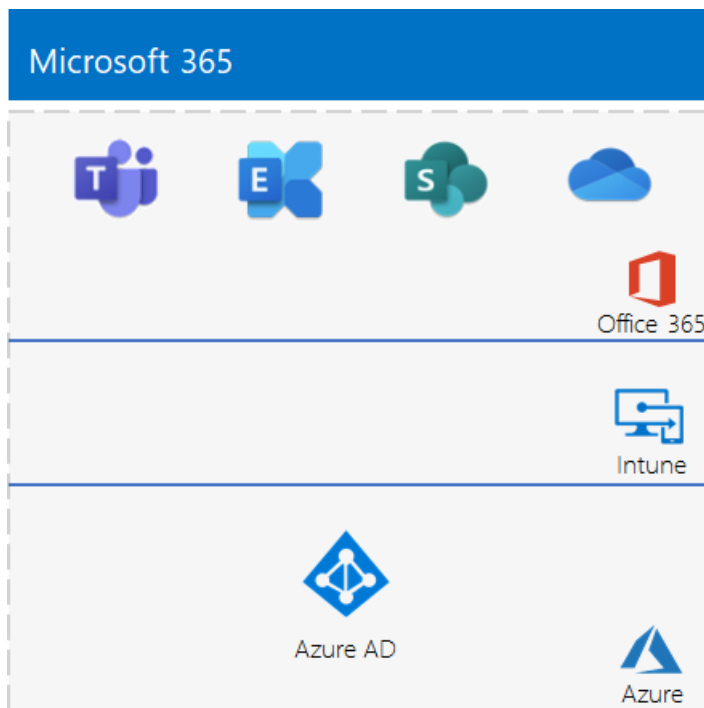
NOTE

The length of the Microsoft 365 E5 trial subscription is 30 days. For a permanent test environment, convert this trial subscription into a paid subscription with a small number of licenses.

Your test environment now has:

- A Microsoft 365 E5 trial subscription.
- All your appropriate user accounts (either just the global administrator or all five user accounts) are enabled to use Microsoft 365 E5.

Your resulting configuration, which adds Microsoft 365 E5, looks like this:



Phase 4: Create a Windows 10 Enterprise computer

In this phase, you create a standalone computer running Windows 10 Enterprise as either a physical computer, a virtual machine, or an Azure virtual machine.

Physical computer

On a personal computer, install Windows 10 Enterprise. You can download the Windows 10 Enterprise trial [here](#).

Virtual machine

Use the hypervisor of your choice to create a virtual machine, and then install Windows 10 Enterprise on it. You can download the Windows 10 Enterprise trial [here](#).

Virtual machine in Azure

To create a Windows 10 virtual machine in Microsoft Azure, *you must have a Visual Studio-based subscription*, which has access to the image for Windows 10 Enterprise. Other types of Azure subscriptions, such as trial and paid subscriptions, do not have access to this image. For the latest information, see [Use Windows client in Azure for dev/test scenarios](#).

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell cmdlets](#). These command sets build a Windows 10 Enterprise virtual machine named WIN10 and all of its required infrastructure, including a resource group, a storage account, and a virtual network. If you are already familiar with Azure infrastructure services, adapt these instructions to suit your currently deployed infrastructure.

First, start a Microsoft PowerShell prompt.

Sign in to your Azure account with this command.

```
Connect-AzAccount
```

Get your subscription name using this command.

```
Get-AzSubscription | Sort Name | Select Name
```

Set your Azure subscription. Replace everything within the quotation marks, including the < and > characters, with the correct name.

```
$subscr="<subscription name>"
Get-AzSubscription -SubscriptionName $subscr | Select-AzSubscription
```

Next, create a new resource group. To determine a unique resource group name, use this command to list your existing resource groups.

```
Get-AzResourceGroup | Sort ResourceGroupName | Select ResourceGroupName
```

Create your new resource group with these commands. Replace everything within the quotation marks, including the < and > characters, with the correct names.

```
$rgName="<resource group name>"
$locName="<location name, such as West US>"
New-AzResourceGroup -Name $rgName -Location $locName
```

Next, create a new virtual network and the WIN10 virtual machine with these commands. When prompted, provide the name and password of the local administrator account for WIN10 and store these in a secure location.

```
$corpnetSubnet=New-AzVirtualNetworkSubnetConfig -Name Corpnet -AddressPrefix 10.0.0.0/24
New-AzVirtualNetwork -Name "M365Ent-TestLab" -ResourceGroupName $rgName -Location $locName -AddressPrefix 10.0.0.0/8 -Subnet $corpnetSubnet
$rule1=New-AzNetworkSecurityRuleConfig -Name "RDPTraffic" -Description "Allow RDP to all VMs on the subnet" -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389
New-AzNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName -Location $locName -SecurityRules $rule1
$vnnet=Get-AzVirtualNetwork -ResourceGroupName $rgName -Name "M365Ent-TestLab"
$nsg=Get-AzNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnnet -Name Corpnet -AddressPrefix "10.0.0.0/24" -NetworkSecurityGroup $nsg
$vnnet | Set-AzVirtualNetwork
$pip=New-AzPublicIpAddress -Name WIN10-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod Dynamic
$nic=New-AzNetworkInterface -Name WIN10-NIC -ResourceGroupName $rgName -Location $locName -SubnetId $vnnet.Subnets[0].Id -PublicIpAddressId $pip.Id
$vm=New-AzVMConfig -VMName WIN10 -VMSize Standard_A2_V2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for WIN10."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName WIN10 -Credential $cred -ProvisionVMAgent -EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsDesktop -Offer Windows-10 -Skus RS3-Pro -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name WIN10-TestLab-OSDisk -DiskSizeInGB 128 -CreateOption FromImage
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Phase 5: Join your Windows 10 computer to Azure AD

After the physical or virtual machine with Windows 10 Enterprise is created, sign in with a local administrator account.

NOTE

For a virtual machine in Azure, use [these instructions](#) to connect to it.

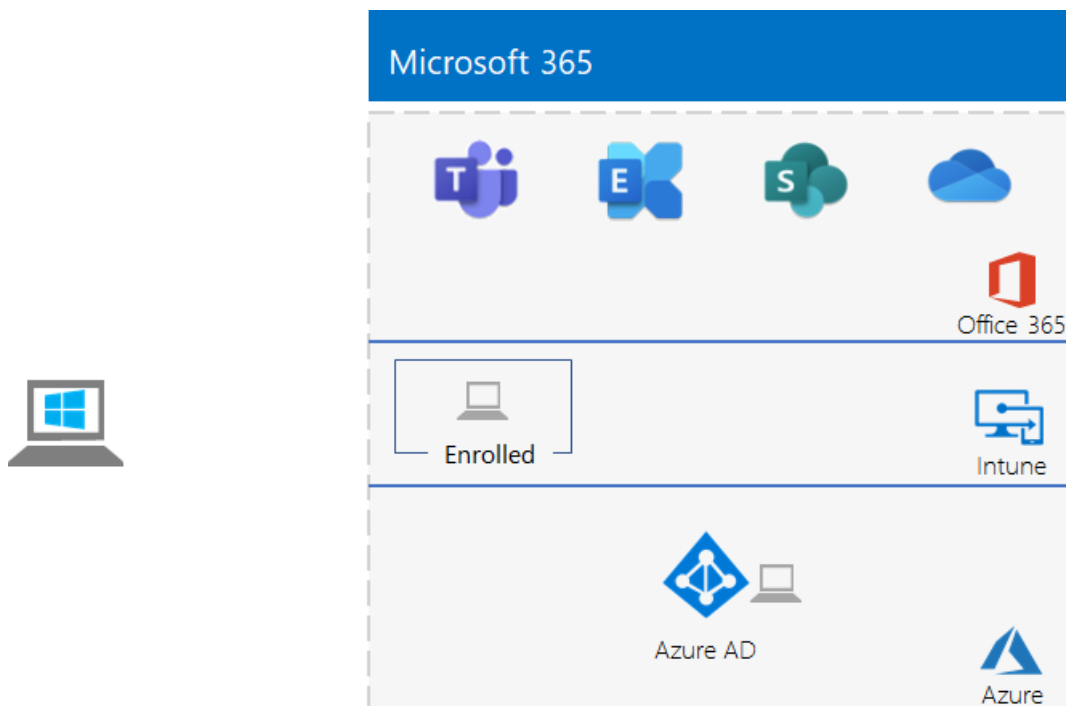
Next, join the WIN10 computer to the Azure AD tenant of your Microsoft 365 E5 subscription.

1. On the desktop of the WIN10 computer, select **Start > Settings > Accounts > Access work or school > Connect**.
2. In the **Set up a work or school account** dialog box, select **Join this device to Azure Active Directory**.
3. In **Work or school account**, enter the global administrator account name of your Microsoft 365 E5 subscription, and then select **Next**.
4. In **Enter password**, enter the password for your global administrator account, and then select **Sign in**.
5. When prompted to make sure that this is your organization, select **Join**, and then select **Done**.
6. Close the settings window.

Next, install Microsoft 365 Apps for enterprise on the WIN10 computer:

1. Open the Microsoft Edge browser and sign in to the [Microsoft 365 admin center](#) with your global administrator account credentials.
2. On the **Microsoft Office Home** tab, select **Install Office**.
3. When prompted with what to do, select **Run**, and then select **Yes** for **User Account Control**.
4. Wait for Office to complete its installation. When you see **You're all set!**, select **Close** twice.

Your resulting environment looks like this:



This includes the WIN10 computer that has:

- Joined the Azure AD tenant of your Microsoft 365 E5 subscription.
- Enrolled as an Azure AD device in Microsoft Intune (EMS).

- Microsoft 365 Apps for enterprise installed.

You are now ready to experiment with additional features of [Microsoft 365 for enterprise](#).

Next steps

Explore these additional sets of Test Lab Guides:

- [Identity](#)
- [Mobile device management](#)
- [Information protection](#)

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

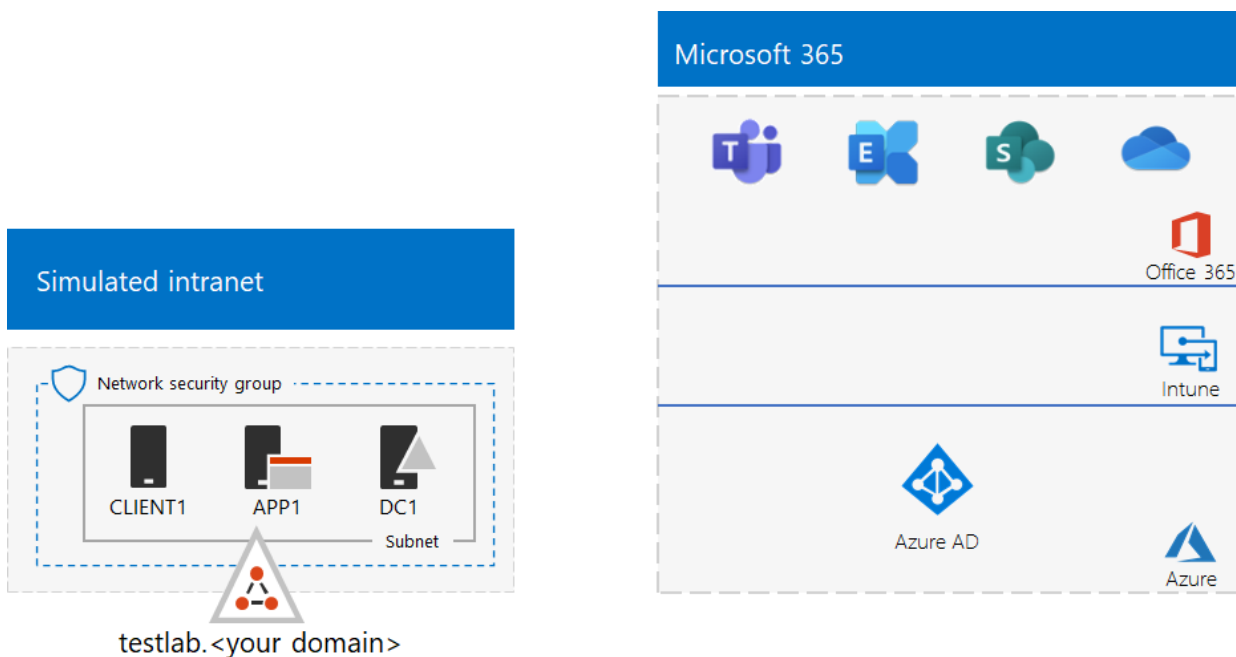
The simulated enterprise base configuration

10/28/2022 • 13 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

This article describes how to create a simplified environment for Microsoft 365 for enterprise that includes:

- A Microsoft 365 E5 trial or paid subscription.
- A simplified organization intranet connected to the internet, consisting of three virtual machines on an Azure virtual network (DC1, APP1, and CLIENT1).



Creating a simplified test environment involves two phases:

- [Phase 1: Create a simulated intranet](#)
- [Phase 2: Create your Microsoft 365 E5 subscription](#)

You can use the resulting environment to test the features and functionality of [Microsoft 365 for enterprise](#) with additional [Test Lab Guides](#) or on your own.



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Create a simulated intranet

In this phase, build a simulated intranet in Azure infrastructure services that includes an Active Directory

Domain Services (AD DS) domain controller, an application server, and a client computer.

You'll use these computers in additional [Microsoft 365 for enterprise Test Lab Guides](#) to configure and demonstrate hybrid identity and other capabilities.

Method 1: Build your simulated intranet with an Azure Resource Manager template

In this method, you use an Azure Resource Manager template to build out the simulated intranet. Azure Resource Manager templates contain all of the instructions to create the Azure networking infrastructure, the virtual machines, and their configuration.

Before deploying the template, read through the [template README page](#) and have the following information ready:

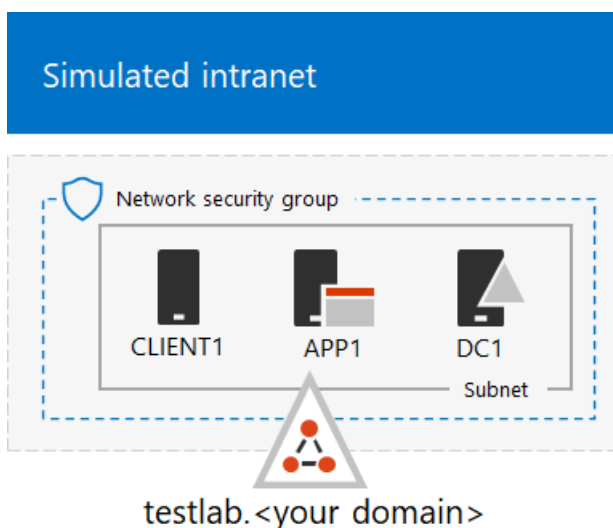
- The public DNS domain name of your test environment (testlab.<your public domain>). You'll enter this name in the **Domain Name** field of the **Custom deployment** page.
- A DNS label prefix for the URLs of the public IP addresses of your virtual machines. You'll need to enter this label in the **Dns Label Prefix** field of the **Custom deployment** page.

After you read through the instructions, select **Deploy to Azure** on the [template README page](#) to get started.

NOTE

The simulated intranet built by the Azure Resource Manager template requires a paid Azure subscription.

After the template is complete, your configuration looks like this:



Method 2: Build your simulated intranet with Azure PowerShell

In this method, you use Windows PowerShell and the Azure PowerShell module to build out the networking infrastructure, the virtual machines, and their configuration.

Use this method if you want to get experience creating elements of Azure infrastructure one step at a time with PowerShell. You can then customize the PowerShell command blocks for your own deployment of other virtual machines in Azure.

Step 1: Create DC1

In this step, you create an Azure virtual network and add DC1, a virtual machine that is a domain controller for an AD DS domain.

First, start a Windows PowerShell command prompt on your local computer.

NOTE

The following command sets use the latest version of Azure PowerShell. See [Get started with Azure PowerShell cmdlets](#).

Sign in to your Azure account with the following command.

```
Connect-AzAccount
```

Get your subscription name using the following command.

```
Get-AzSubscription | Sort Name | Select Name
```

Set your Azure subscription. Replace everything within the quotation marks, including the angle brackets ("**<**" and "**>**"), with the correct name.

```
$subscr="<subscription name>"  
Get-AzSubscription -SubscriptionName $subscr | Select-AzSubscription
```

Next, create a new resource group for your simulated enterprise test lab. To determine a unique resource group name, use this command to list your existing resource groups.

```
Get-AzResourceGroup | Sort ResourceGroupName | Select ResourceGroupName
```

Create your new resource group with these commands. Replace everything within the quotation marks, including the angle brackets, with the correct names.

```
$rgName="<resource group name>"  
$locName="<location name, such as West US>"  
New-AzResourceGroup -Name $rgName -Location $locName
```

Next, create the TestLab virtual network that will host the corporate network subnet of the simulated enterprise environment and protect it with a network security group. Fill in the name of your resource group and run these commands at the PowerShell command prompt on your local computer.

```
$rgName="<name of your new resource group>"  
$locName=(Get-AzResourceGroup -Name $rgName).Location  
$corpnetSubnet=New-AzVirtualNetworkSubnetConfig -Name Corpnet -AddressPrefix 10.0.0.0/24  
New-AzVirtualNetwork -Name TestLab -ResourceGroupName $rgName -Location $locName -AddressPrefix 10.0.0.0/8 -  
Subnet $corpnetSubnet -DNSServer 10.0.0.4  
$rule1=New-AzNetworkSecurityRuleConfig -Name "RDPTraffic" -Description "Allow RDP to all VMs on the subnet"  
-Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange  
* -DestinationAddressPrefix * -DestinationPortRange 3389  
New-AzNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName -Location $locName -SecurityRules $rule1  
$vnet=Get-AzVirtualNetwork -ResourceGroupName $rgName -Name TestLab  
$nsg=Get-AzNetworkSecurityGroup -Name Corpnet -ResourceGroupName $rgName  
Set-AzVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name Corpnet -AddressPrefix "10.0.0.0/24" -  
NetworkSecurityGroup $nsg  
$vnet | Set-AzVirtualNetwork
```

Next, you create the DC1 virtual machine and configure it as a domain controller for the **testlab.<your public domain>** AD DS domain and a DNS server for the virtual machines of the TestLab virtual network. For example, if your public domain name is **contoso.com**, the DC1 virtual machine will be a domain controller for the **testlab.contoso.com** domain.

To create an Azure virtual machine for DC1, fill in the name of your resource group and run these commands at the PowerShell command prompt on your local computer.

```
$rgName="<resource group name>"
$locName=(Get-AzResourceGroup -Name $rgName).Location
$vnet=Get-AzVirtualNetwork -Name TestLab -ResourceGroupName $rgName
$pip=New-AzPublicIpAddress -Name DC1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod
Dynamic
$nic=New-AzNetworkInterface -Name DC1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId
$vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -PrivateIpAddress 10.0.0.4
$vm=New-AzVMConfig -VMName DC1 -VMSize Standard_A2_V2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for DC1."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName DC1 -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name "DC1-OS" -DiskSizeInGB 128 -CreateOption FromImage
$diskConfig=New-AzDiskConfig -AccountType "Standard_LRS" -Location $locName -CreateOption Empty -DiskSizeGB
20
$dataDisk1=New-AzDisk -DiskName "DC1-DataDisk1" -Disk $diskConfig -ResourceGroupName $rgName
$vm=Add-AzVMDataDisk -VM $vm -Name "DC1-DataDisk1" -CreateOption Attach -ManagedDiskId $dataDisk1.Id -Lun 1
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

You will be prompted for a user name and password for the local administrator account on DC1. Use a strong password and record both the name and password in a secure location.

Next, connect to the DC1 virtual machine:

1. In the [Azure portal](#), select **Resource Groups** > *<the name of your new resource group>* > **DC1** > **Connect**.
2. In the open pane, select **Download RDP file**. Open the DC1.rdp file that is downloaded, and then select **Connect**.
3. Specify the DC1 local administrator account name:
 - For Windows 7:
In the **Windows Security** dialog box, select **Use another account**. In **User name**, enter **DC1\<local administrator account name>**.
 - For Windows 8 or Windows 10:
In the **Windows Security** dialog box, select **More choices**, and then select **Use a different account**. In **User name**, enter **DC1\<local administrator account name>**.
4. In **Password**, enter the password of the local administrator account, and then select **OK**.
5. When prompted, select **Yes**.

Next, add an extra data disk as a new volume with the drive letter F: with this command at an administrator-level Windows PowerShell command prompt on DC1.

```
Get-Disk | Where PartitionStyle -eq "RAW" | Initialize-Disk -PartitionStyle MBR -PassThru | New-Partition -
AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS -NewFileSystemLabel "WSAD Data"
```

Next, configure DC1 as a domain controller and DNS server for the **testlab.<your public domain>** domain. Specify your public domain name, remove the angle brackets, and then run these commands at an administrator-level Windows PowerShell command prompt on DC1.

```
$yourDomain="<your public domain>"
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Install-ADDSForest -DomainName testlab.$yourDomain -DatabasePath "F:\NTDS" -SysvolPath "F:\SYSVOL" -LogPath
"F:\Logs"
```

You will need to specify a safe mode administrator password. Store this password in a secure location.

Note that these commands can take a few minutes to complete.

After DC1 restarts, reconnect to the DC1 virtual machine.

1. In the [Azure portal](#), select **Resource Groups** > *<your resource group name>* > **DC1** > **Connect**.
2. Run the DC1.rdp file that is downloaded, and then select **Connect**.
3. In **Windows Security**, select **Use another account**. In **User name**, enter **TESTLAB\<local administrator account name>**.
4. In the **Password** box, enter the password of the local administrator account, and then select **OK**.
5. When prompted, select **Yes**.

Next, create a user account in Active Directory that will be used when signing in to TESTLAB domain member computers. Run this command at an administrator-level Windows PowerShell command prompt.

```
New-ADUser -SamAccountName User1 -AccountPassword (read-host "Set user password" -assecurestring) -name
"User1" -enabled $true -PasswordNeverExpires $true -ChangePasswordAtLogon $false
```

Note that this command prompts you to supply the User1 account password. This account will be used for remote desktop connections for all TESTLAB domain member computers, so choose a strong password. Record the User1 account password and store it in a secured location.

Next, configure the new User1 account as a domain, enterprise, and schema administrator. Run this command at the administrator-level Windows PowerShell command prompt.

```
$yourDomain="<your public domain>"
$domainName = "testlab."+$yourDomain
$username="user1@" + $domainName
$userSID=(New-Object
System.Security.Principal.NTAccount($username)).Translate([System.Security.Principal.SecurityIdentifier]).Va
lue
$groupNames=@("Domain Admins","Enterprise Admins","Schema Admins")
ForEach ($name in $groupNames) {Add-ADPrincipalGroupMembership -Identity $userSID -MemberOf (Get-ADGroup -
Identity $name).SID.Value}
```

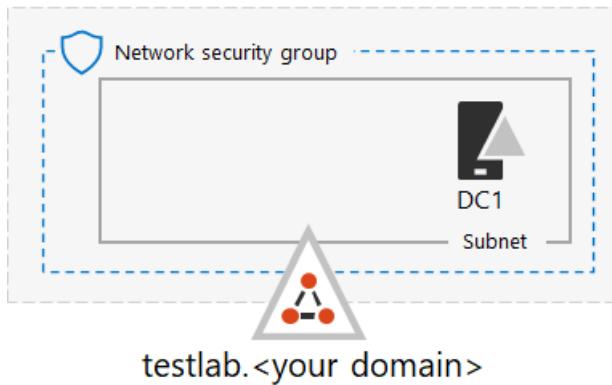
Close the Remote Desktop session with DC1 and then reconnect using the TESTLAB\User1 account.

Next, to allow traffic for the Ping tool, run this command at an administrator-level Windows PowerShell command prompt.

```
Set-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)" -enabled True
```

Your current configuration looks like this:

Simulated intranet



Step 2: Configure APP1

In this step, you create and configure APP1, which is an application server that initially provides web and file sharing services.

To create an Azure Virtual Machine for APP1, fill in the name of your resource group and run these commands at the command prompt on your local computer.

```
$rgName="<resource group name>"
$locName=(Get-AzResourceGroup -Name $rgName).Location
$vnet=Get-AzVirtualNetwork -Name TestLab -ResourceGroupName $rgName
$pip=New-AzPublicIpAddress -Name APP1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod
Dynamic
$nic=New-AzNetworkInterface -Name APP1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId
$vnet.Subnets[0].Id -PublicIpAddressId $pip.Id
$vm=New-AzVMConfig -VMName APP1 -VMSize Standard_A2_V2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for APP1."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName APP1 -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name "APP1-OS" -DiskSizeInGB 128 -CreateOption FromImage
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Next, connect to the APP1 virtual machine using the APP1 local administrator account name and password, and then open a Windows PowerShell command prompt.

To check name resolution and network communication between APP1 and DC1, run the **ping dc1.testlab.<your public domain name>** command and verify that there are four replies.

Next, join the APP1 virtual machine to the TESTLAB domain with these commands at the Windows PowerShell prompt.

```
$yourDomain="<your public domain name>"
Add-Computer -DomainName ("testlab." + $yourDomain)
Restart-Computer
```

Note that you after you run the **Add-Computer** command, you must supply the TESTLAB\User1 domain account credentials.

After APP1 restarts, connect to it using the TESTLAB\User1 account, and then open an administrator-level Windows PowerShell command prompt.

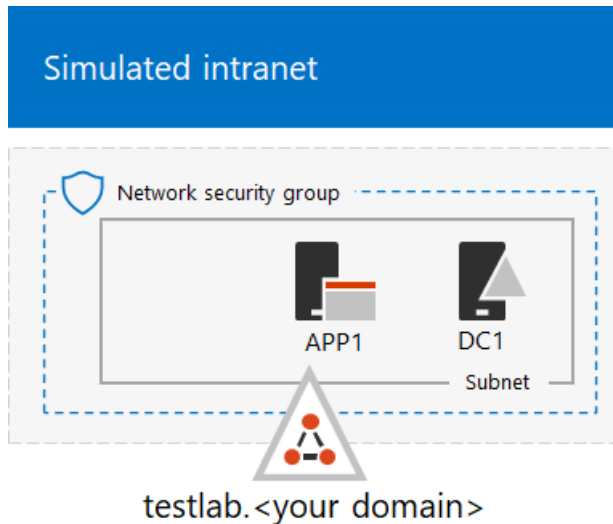
Next, make APP1 a web server with this command at an administrator-level Windows PowerShell command prompt on APP1.

```
Install-WindowsFeature Web-WebServer -IncludeManagementTools
```

Next, create a shared folder and a text file within the folder on APP1 with these PowerShell commands.

```
New-Item -path c:\files -type directory  
Write-Output "This is a shared file." | out-file c:\files\example.txt  
New-SmbShare -name files -path c:\files -changeaccess TESTLAB\User1
```

Your current configuration looks like this:



Step 3: Configure CLIENT1

In this step, you create and configure CLIENT1, which acts as a typical laptop, tablet, or desktop computer on the intranet.

NOTE

The following command set creates CLIENT1 running Windows Server 2016 Datacenter, which can be done for all types of Azure subscriptions. If you have a Visual Studio-based Azure subscription, you can create CLIENT1 running Windows 10 with the [Azure portal](#).

To create an Azure Virtual Machine for CLIENT1, fill in the name of your resource group and run these commands at the command prompt on your local computer.

```

$rgName="<resource group name>"
$locName=(Get-AzResourceGroup -Name $rgName).Location
$vnet=Get-AzVirtualNetwork -Name TestLab -ResourceGroupName $rgName
$pip=New-AzPublicIpAddress -Name CLIENT1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod
Dynamic
$nic=New-AzNetworkInterface -Name CLIENT1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId
$vnet.Subnets[0].Id -PublicIpAddressId $pip.Id
$vm=New-AzVMConfig -VMName CLIENT1 -VMSize Standard_A2_V2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for CLIENT1."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName CLIENT1 -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name "CLIENT1-OS" -DiskSizeInGB 128 -CreateOption FromImage
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

```

Next, connect to the CLIENT1 virtual machine using the CLIENT1 local administrator account name and password, and then open an administrator-level Windows PowerShell command prompt.

To check name resolution and network communication between CLIENT1 and DC1, run the **ping dc1.testlab.<your public domain name>** command at a Windows PowerShell command prompt and verify that there are four replies.

Next, join the CLIENT1 virtual machine to the TESTLAB domain with these commands at the Windows PowerShell prompt.

```

$yourDomain="<your public domain name>"
Add-Computer -DomainName ("testlab." + $yourDomain)
Restart-Computer

```

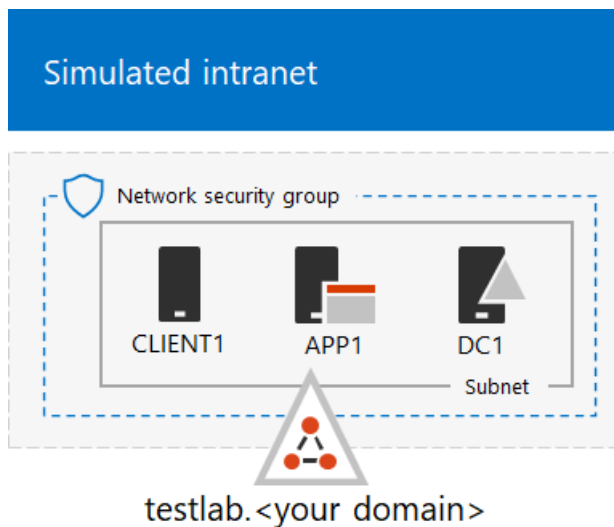
Note that you must supply your TESTLAB\User1 domain account credentials after running the **Add-Computer** command.

After CLIENT1 restarts, connect to it using the TESTLAB\User1 account name and password, and then open an administrator-level Windows PowerShell command prompt.

Next, verify that you can access web and file share resources on APP1 from CLIENT1.

1. In Server Manager, in the tree pane, select **Local Server**.
2. In **Properties** for **CLIENT1**, select **On** next to **IE Enhanced Security Configuration**.
3. In **Internet Explorer Enhanced Security Configuration**, select **Off** for **Administrators and Users**, and then select **OK**.
4. From the Start screen, select **Internet Explorer**, and then select **OK**.
5. In the address bar, enter **http://app1.testlab.<your public domain name>/**, and then press **Enter**. You should see the default Internet Information Services web page for APP1.
6. On the desktop taskbar, select the File Explorer icon.
7. In the address bar, enter **\\app1\Files**, and then press **Enter**. You should see a folder window with the contents of the Files shared folder.
8. In the **Files** shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file.
9. Close the **example.txt - Notepad** and the **Files** shared folder windows.

Your current configuration looks like this:



Phase 2: Create your Microsoft 365 E5 subscription

In this phase, you create a new Microsoft 365 E5 subscription that uses a new Azure AD tenant, one that is separate from your production subscription. You can do this in two ways:

- Use a trial subscription of Microsoft 365 E5.

The Microsoft 365 E5 trial subscription is 30 days, which can be easily extended to 60 days. When the trial subscription expires, you must either convert it to a paid subscription or create a new trial subscription. Creating new trial subscriptions means you will leave your configuration, which could include complex scenarios, behind.

- Use a separate production subscription of Microsoft 365 E5 with a small number of licenses.

This is an additional cost, but ensures that you have a working test environment that doesn't expire; in it, you can try features, configurations, and scenarios. You can use the same test environment over the long term for proofs of concept, demonstration to peers and management, and application development and testing. This is the recommended method.

Sign up for an Office 365 E5 trial subscription

From the Azure portal, connect to CLIENT1 with the CORP\User1 account.

To create a new Office 365 E5 trial subscription, perform the instructions in [Phase 1](#) of the lightweight base configuration Test Lab Guide.

To configure your new Office 365 E5 trial subscription, perform the instructions in [Phase 2](#) of the lightweight base configuration Test Lab Guide.

Using an Office 365 E5 test environment

If you need only an Office 365 test environment, you do not need to read the rest of this article.

For additional Test Lab Guides that apply to both Microsoft 365 and Office 365, see [Microsoft 365 for enterprise Test Lab Guides](#).

Add a Microsoft 365 E5 trial subscription

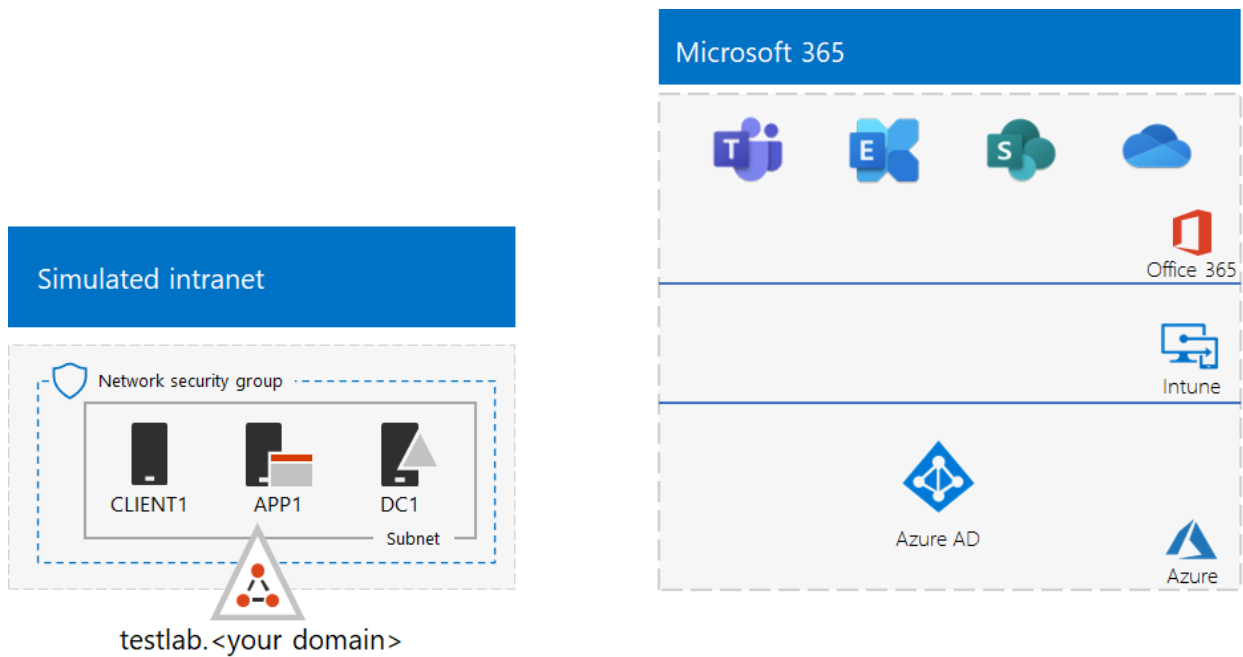
To add a Microsoft 365 E5 trial subscription and configure your users accounts with licenses, perform the instructions in [Phase 3](#) of the lightweight base configuration Test Lab Guide.

Results

Your test environment now has:

- Microsoft 365 E5 trial subscription.
- All your appropriate user accounts are enabled to use Microsoft 365 E5.
- A simulated and simplified intranet.

Your final configuration looks like this:



You are now ready to experiment with additional features of [Microsoft 365 for enterprise](#).

Next steps

Explore these additional sets of Test Lab Guides:

- [Identity](#)
- [Mobile device management](#)
- [Information protection](#)

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

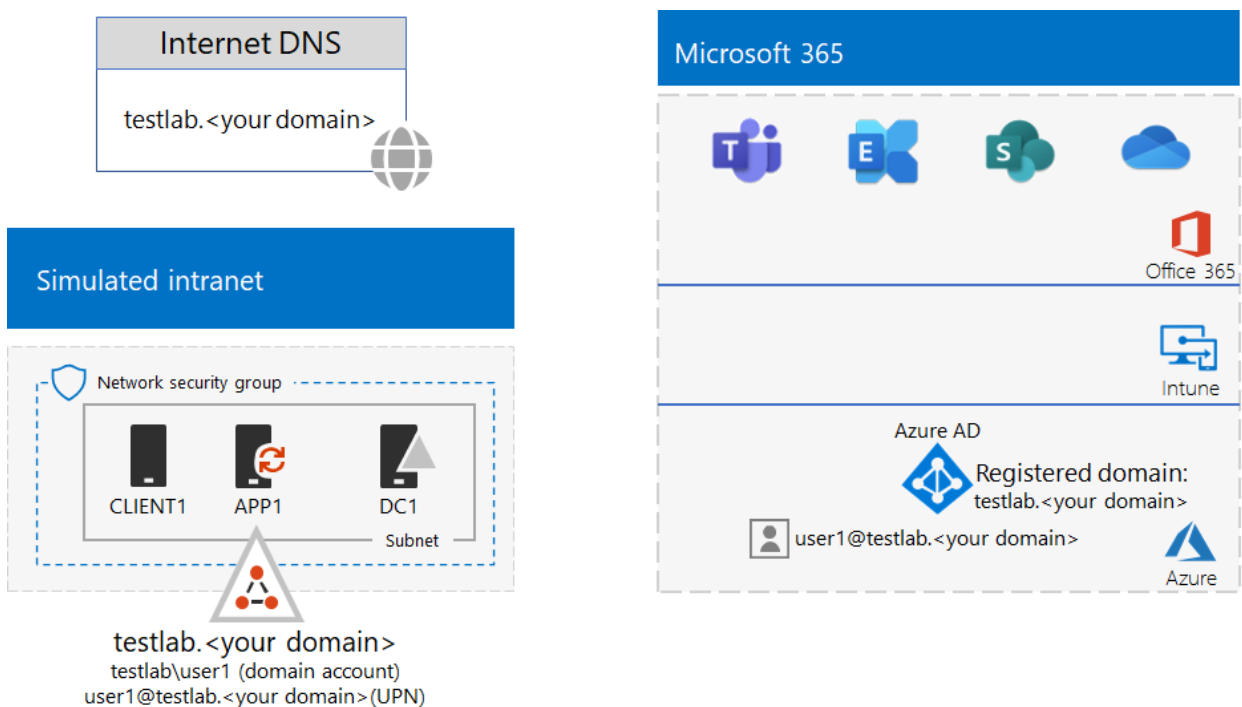
Password hash synchronization for your Microsoft 365 test environment

10/28/2022 • 4 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

Many organizations use Azure AD Connect and password hash synchronization to synchronize the set of accounts in their on-premises Active Directory Domain Services (AD DS) forest to the set of accounts in the Azure AD tenant of their Microsoft 365 subscription.

This article describes how you can add password hash synchronization to your Microsoft 365 test environment, which results in this configuration:



Setting up this test environment involves three phases:

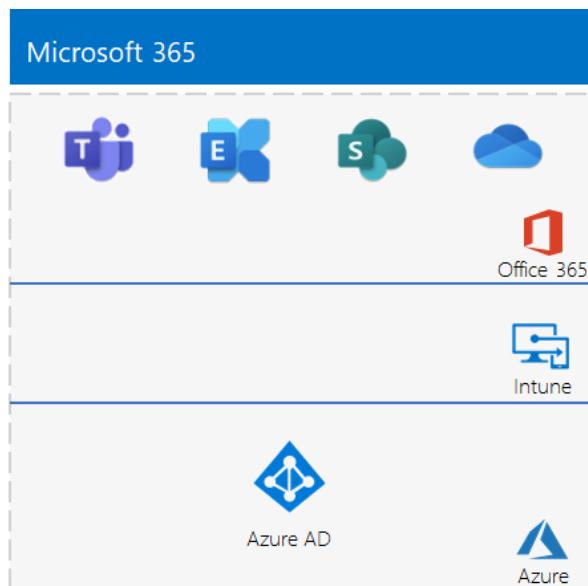
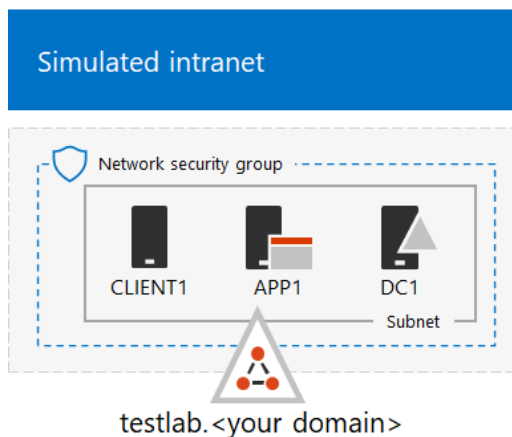
- [Phase 1: Create the Microsoft 365 simulated enterprise test environment](#)
- [Phase 2: Create and register the testlab domain](#)
- [Phase 3: Install Azure AD Connect on APP1](#)

TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Create the Microsoft 365 simulated enterprise test environment

Follow the instructions in [simulated enterprise base configuration for Microsoft 365](#). Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscription.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines in an Azure virtual network. DC1 is a domain controller for the testlab.<your public domain name> AD DS domain.

Phase 2: Create and register the testlab domain

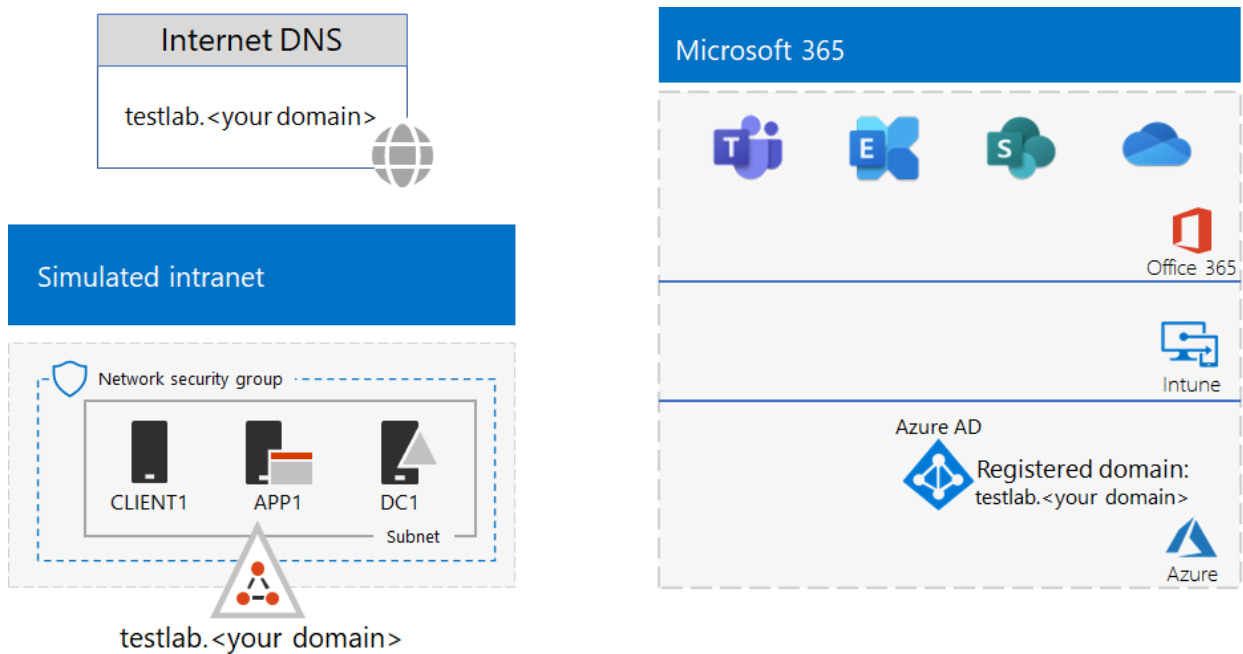
In this phase, add a public DNS domain, and then add it to your subscription.

First, work with your public DNS registration provider to create a new public DNS domain name that's based on your current domain name, and then add it to your subscription. We recommend using the name **testlab**.

<your public domain>. For example, if your public domain name is **contoso.com**, add the public domain name: **testlab.contoso.com**.

Next, add the **testlab.<your public domain>** domain to your Microsoft 365 trial or paid subscription by going through the domain registration process. This consists of adding additional DNS records to the **testlab.<your public domain>** domain. For more information, see [Add a domain to Microsoft 365](#).

Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscription with the DNS domain testlab.<your public domain name> registered.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.

Notice how the testlab.<your public domain name> is now:

- Supported by public DNS records.
- Registered in your Microsoft 365 subscriptions.
- The AD DS domain on your simulated intranet.

Phase 3: Install Azure AD Connect on APP1

In this phase, install and configure the Azure AD Connect tool on APP1, and then verify that it works.

First, install and configure Azure AD Connect on APP1.

1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, open an administrator-level Windows PowerShell command prompt, and then run these commands to disable Internet Explorer Enhanced Security:

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}" -Name "IsInstalled" -Value 0
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A8-37EF-4b3f-8CFC-4F3A74704073}" -Name "IsInstalled" -Value 0
Stop-Process -Name Explorer -Force
```

3. From the taskbar, select **Internet Explorer** and go to <https://aka.ms/aadconnect>.
4. On the Microsoft Azure Active Directory Connect page, select **Download**, and then select **Run**.
5. On the **Welcome to Azure AD Connect** page, select **I agree**, and then select **Continue**.
6. On the **Express Settings** page, select **Use express settings**.

7. On the **Connect to Azure AD** page, enter your global administrator account name in **Username**, enter its password in **Password**, and then select **Next**.
8. On the **Connect to AD DS** page, enter TESTLAB\User1 in **Username**, enter its password in **Password**, and then select **Next**.
9. On the **Ready to configure** page, select **Install**.
10. On the **Configuration complete** page, select **Exit**.
11. In Internet Explorer, go to the Microsoft 365 admin center (<https://portal.microsoft.com>).
12. In the left navigation pane, select **Users > Active users**.

Note the account named **User1**. This account is from the TESTLAB AD DS domain and is proof that directory synchronization has worked.

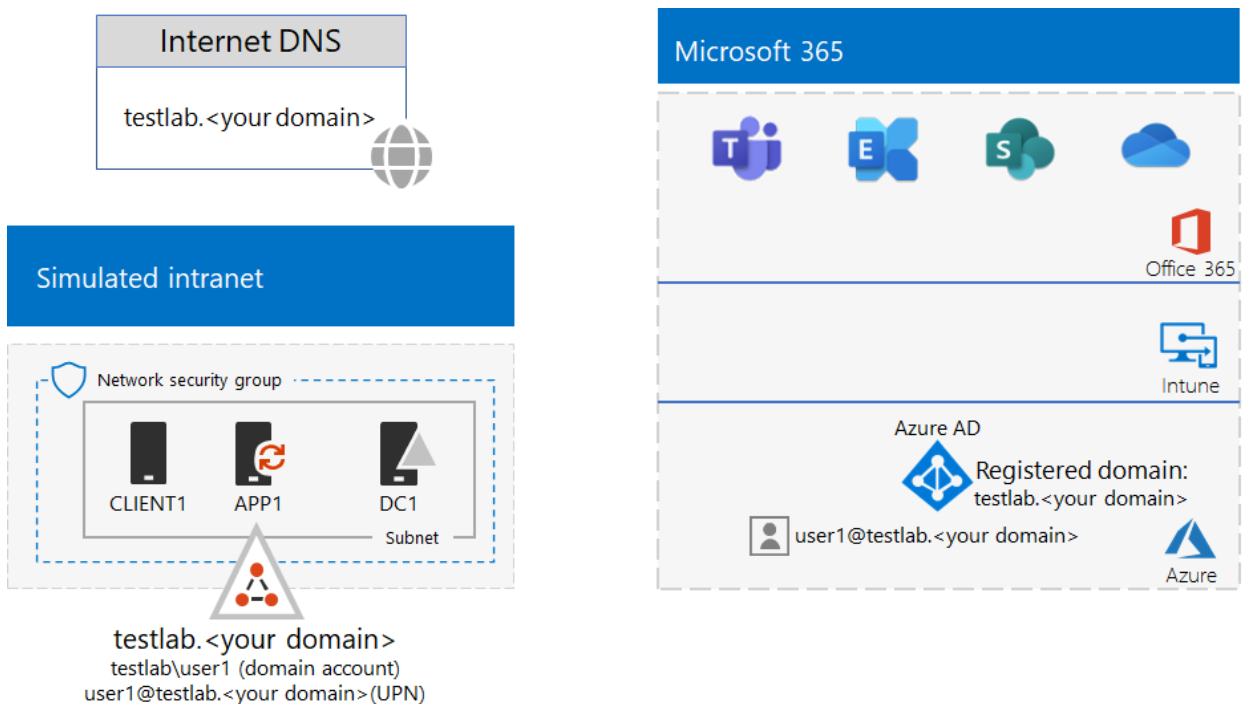
13. Select the **User1** account, and then select **Licenses and apps**.
14. In **Product licenses**, select your location (if needed), disable the **Office 365 E5** license, and then enable the **Microsoft 365 E5** license.
15. Select **Save** at the bottom of the page, and then select **Close**.

Next, test the ability to sign in to your subscription with the **user1@testlab.<your domain name>** user name of the User1 account:

1. From APP1, sign out, and then sign in again, this time specifying a different account.
2. When prompted for a user name and password, specify **user1@testlab.<your domain name>** and the User1 password. You should successfully sign in as User1.

Notice that although User1 has domain administrator permissions for the TESTLAB AD DS domain, it is not a global administrator. Therefore, you will not see the **Admin** icon as an option.

Your resulting configuration looks like this:



This configuration consists of:

- Microsoft 365 E5 or Office 365 E5 trial or paid subscriptions with the DNS domain TESTLAB.<your domain

name> registered.

- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. Azure AD Connect runs on APP1 to periodically synchronize the TESTLAB AD DS domain to the Azure AD tenant of your Microsoft 365 subscription.
- The User1 account in the TESTLAB AD DS domain has been synchronized with the Azure AD tenant.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

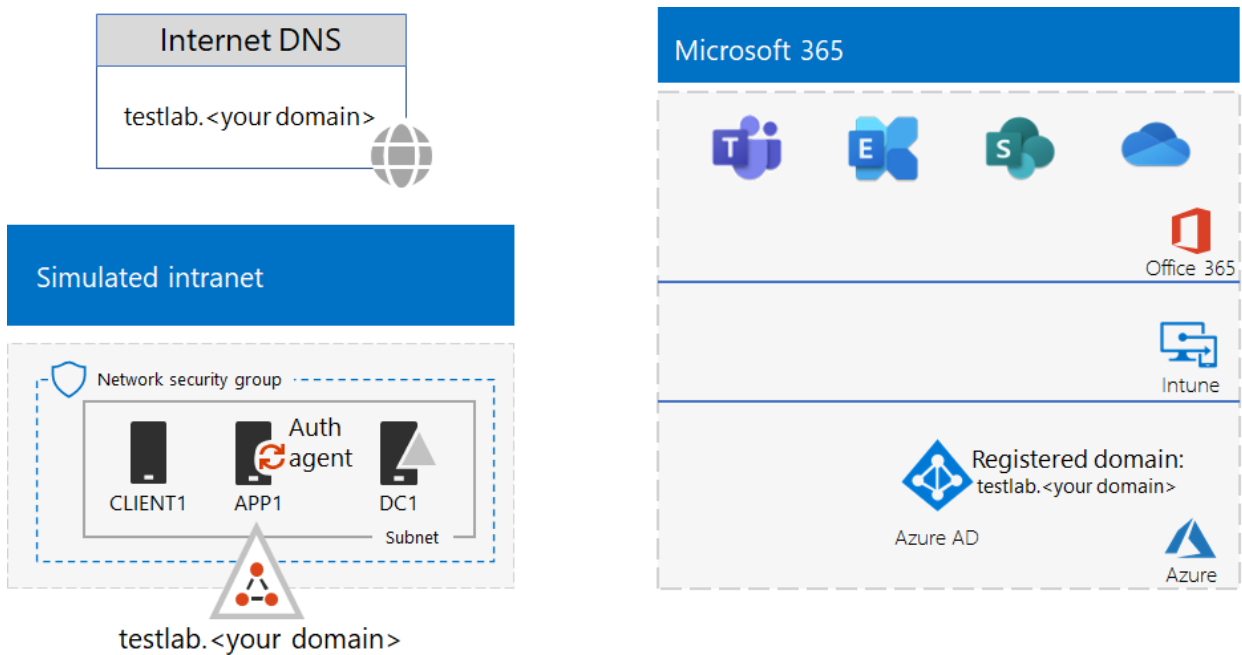
[Microsoft 365 for enterprise documentation](#)

Pass-through authentication for your Microsoft 365 test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

Organizations that want to directly use their on-premises Active Directory Domain Services (AD DS) infrastructure for authentication to Microsoft cloud-based services and applications can use pass-through authentication. This article describes how you can configure your Microsoft 365 test environment for pass-through authentication, resulting in the following configuration:



There are two phases to setting up this test environment:

1. Create the Microsoft 365 simulated enterprise test environment with password hash synchronization.
2. Configure Azure AD Connect on APP1 for pass-through authentication.

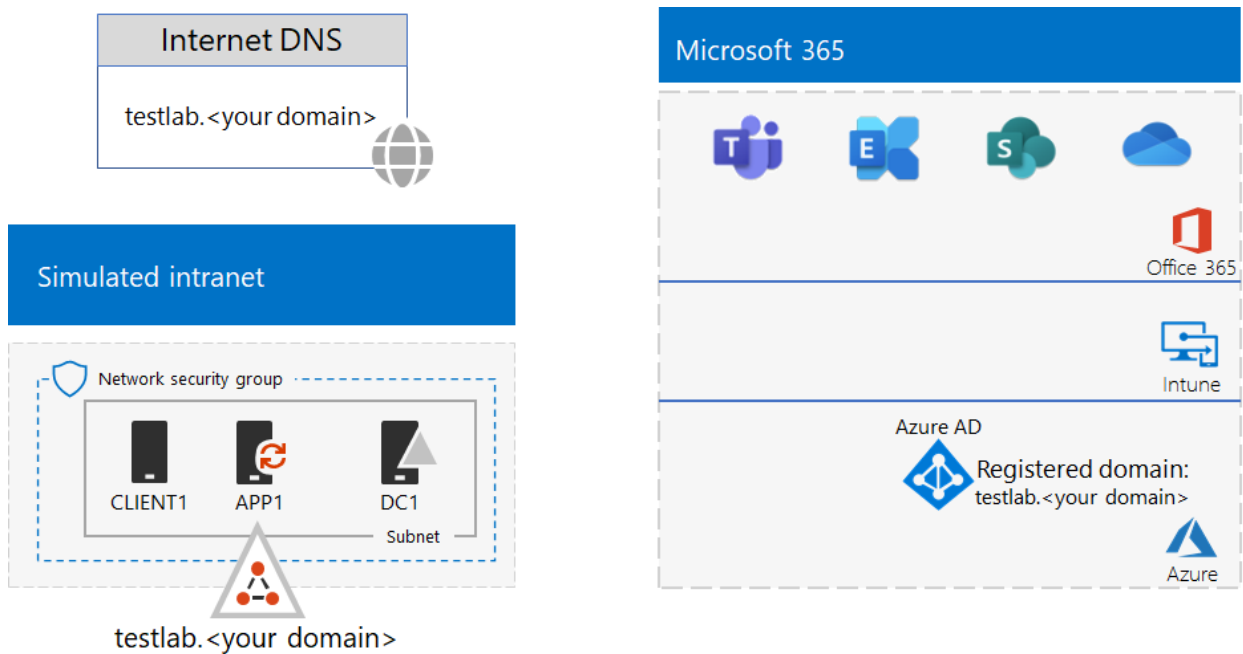


TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack.

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

Follow the instructions in [password hash synchronization for Microsoft 365](#). Here is your resulting configuration.



This configuration consists of:

- Microsoft 365 E5 trial or paid subscription.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. Azure AD Connect runs on APP1 to synchronize the TESTLAB AD DS domain to the Azure AD tenant of your Microsoft 365 subscription periodically.

Phase 2: Configure Azure AD Connect on APP1 for pass-through authentication

In this phase, you configure Azure AD Connect on APP1 to use pass-through authentication, and then verify that it works.

Configure Azure AD Connect on APP1

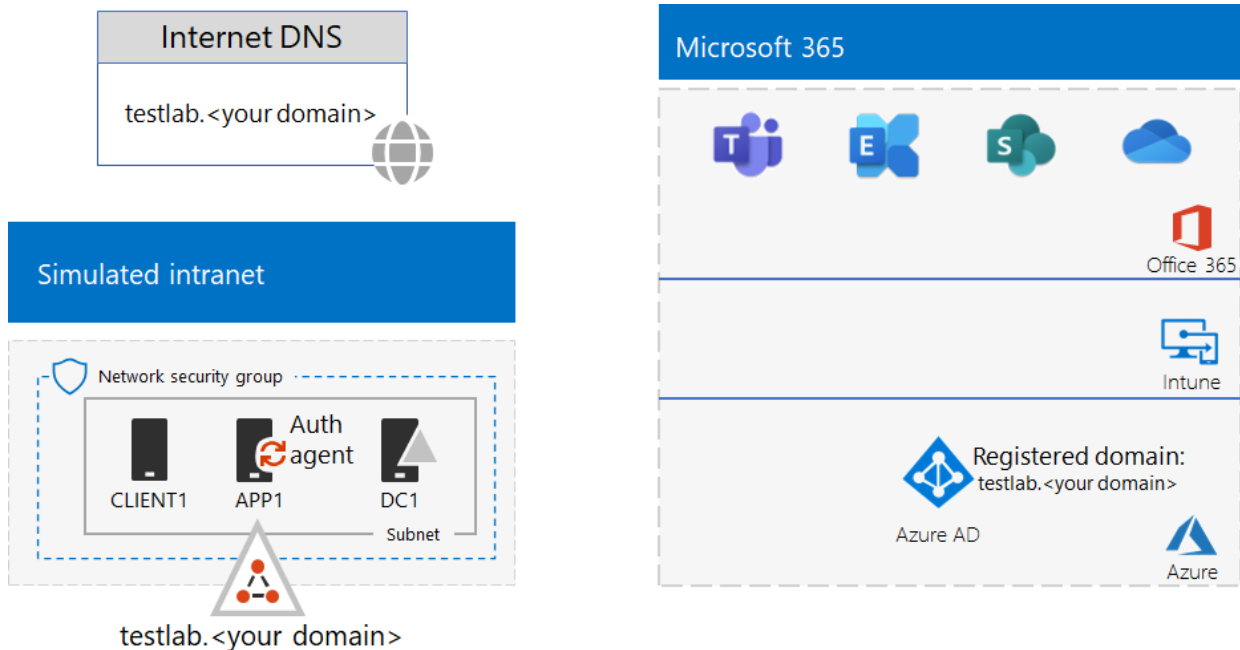
1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, run Azure AD Connect.
3. On the **Welcome** page, click **Configure**.
4. On the Additional tasks page, click **Change user sign-in**, and then click **Next**.
5. On the **Connect to Azure AD** page, type your global administrator account credentials, and then click **Next**.
6. On the **User sign-in** page, click **Pass-through authentication**, and then click **Next**.
7. On the **Ready to configure** page, click **Configure**.
8. On the **Configuration complete** page, click **Exit**.
9. From the Azure portal, in the left pane, click **Azure Active Directory** > **Azure AD Connect**. Verify that the **Pass-through authentication** feature appears as **Enabled**.
10. Click **Pass-through authentication**. The **Pass-through authentication** pane lists the servers where your Authentication Agents are installed. You should see APP1 in the list. Close the **Pass-through authentication** pane.

Next, test the ability to sign in to your subscription with the **user1@testlab.<your public domain>** user name of the User1 account.

1. From APP1, sign out, and then sign in again, this time specifying a different account.
2. When prompted for a user name and password, specify **user1@testlab.<your public domain>** and the User1 password. You should successfully sign in as User1.

Notice that although User1 has domain administrator permissions for the TESTLAB AD DS domain, it is not a global administrator. Therefore, you will not see the **Admin** icon as an option.

Here is your resulting configuration:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscriptions with the DNS domain `testlab.<your domain name>` registered.
- A simplified organization intranet connected to the Internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. An Authentication Agent runs on APP1 to handle pass-through authentication requests from the Azure AD tenant of your Microsoft 365 subscription.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

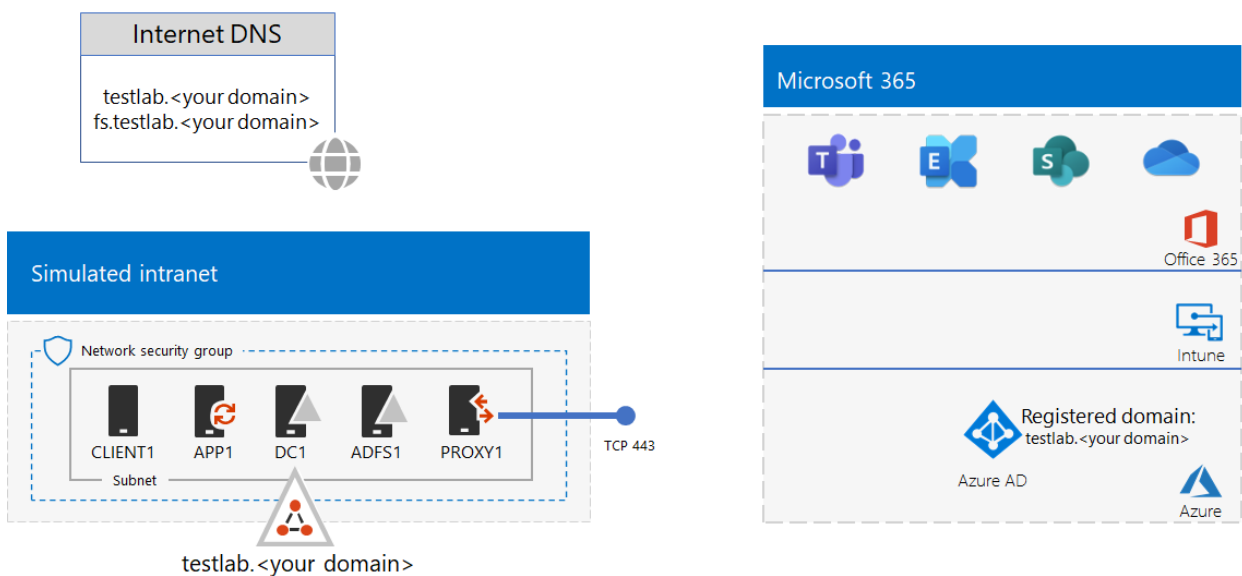
Federated identity for your Microsoft 365 test environment

10/28/2022 • 13 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

Microsoft 365 supports federated identity. This means that instead of performing the validation of credentials itself, Microsoft 365 refers the connecting user to a federated authentication server that Microsoft 365 trusts. If the user's credentials are correct, the federated authentication server issues a security token that the client then sends to Microsoft 365 as proof of authentication. Federated identity allows for the offloading and scaling up of authentication for a Microsoft 365 subscription and advanced authentication and security scenarios.

This article describes how to configure federated authentication for your Microsoft 365 test environment, resulting in the following:



This configuration consists of:

- A Microsoft 365 E5 trial or production subscription.
- A simplified organization intranet connected to the internet, consisting of five virtual machines on a subnet of an Azure virtual network (`DC1`, `APP1`, `CLIENT1`, `ADFS1`, and `PROXY1`). Azure AD Connect runs on `APP1` to synchronize the list of accounts in the Active Directory Domain Services domain to Microsoft 365. `PROXY1` receives the incoming authentication requests. `ADFS1` validates credentials with `DC1` and issues security tokens.

Setting up this test environment involves five phases:

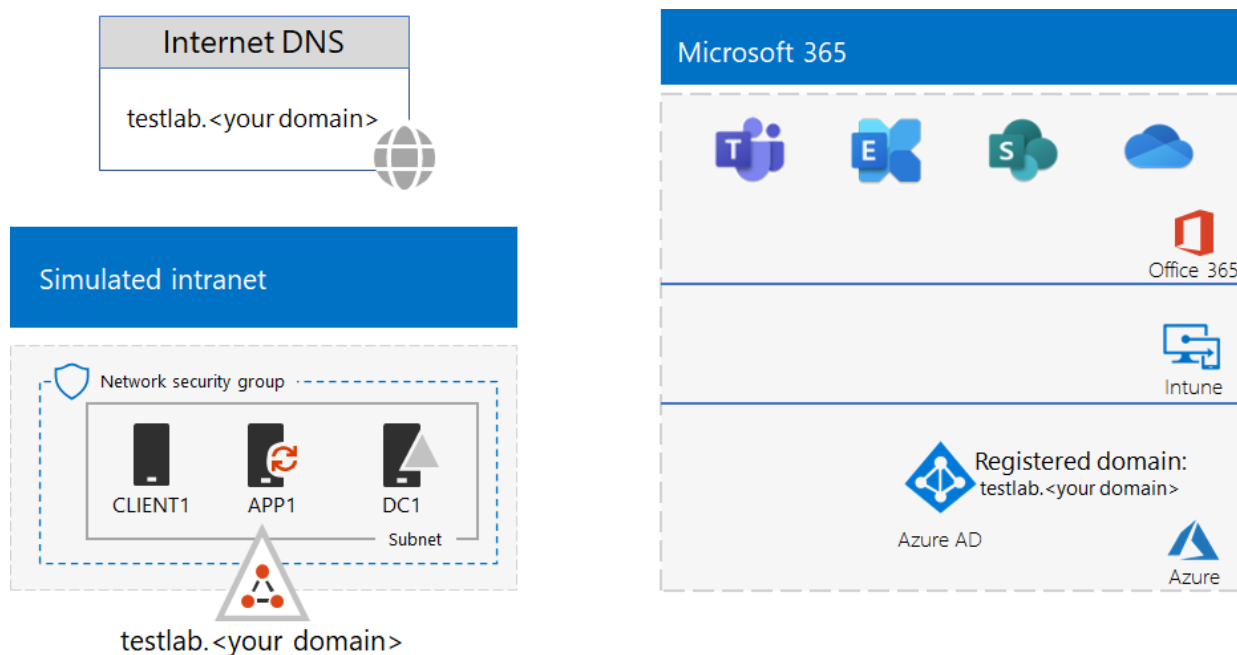
- [Phase 1: Configure password hash synchronization for your Microsoft 365 test environment](#)
- [Phase 2: Create the AD FS server](#)
- [Phase 3: Create the web proxy server](#)
- [Phase 4: Create a self-signed certificate and configure ADFS1 and PROXY1](#)
- [Phase 5: Configure Microsoft 365 for federated identity](#)

NOTE

You can't configure this test environment with an Azure Trial subscription.

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

Follow the instructions in [password hash synchronization for Microsoft 365](#). Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscriptions.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network. Azure AD Connect runs on APP1 to synchronize the TESTLAB Active Directory Domain Services (AD DS) domain to the Azure AD tenant of your Microsoft 365 subscriptions periodically.

Phase 2: Create the AD FS server

An AD FS server provides federated authentication between Microsoft 365 and the accounts in the corp.contoso.com domain hosted on DC1.

To create an Azure virtual machine for ADFS1, fill in the name of your subscription and the resource group and Azure location for your Base Configuration, and then run these commands at the Azure PowerShell command prompt on your local computer.

```

$subscrName="<your Azure subscription name>"
$rgName="<the resource group name of your Base Configuration>"
$vnetName="TlgBaseConfig-01-VNET"
# NOTE: If you built your simulated intranet with Azure PowerShell, comment the previous line with a "#" and
remove the "#" from the next line.
#$vnetName="TestLab"
Connect-AzAccount
Select-AzSubscription -SubscriptionName $subscrName
$staticIP="10.0.0.100"
$locName=(Get-AzResourceGroup -Name $rgName).Location
$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
$pip = New-AzPublicIpAddress -Name ADFS1-PIP -ResourceGroupName $rgName -Location $locName -AllocationMethod
Dynamic
$nic = New-AzNetworkInterface -Name ADFS1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId
$vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName ADFS1 -VMSize Standard_D2_v2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for ADFS1."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName ADFS1 -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name "ADFS-OS" -DiskSizeInGB 128 -CreateOption FromImage -StorageAccountType
"Standard_LRS"
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm

```

Next, use the [Azure portal](#) to connect to the ADFS1 virtual machine using the ADFS1 local administrator account name and password, and then open a Windows PowerShell command prompt.

To check name resolution and network communication between ADFS1 and DC1, run the **ping dc1.corp.contoso.com** command and check that there are four replies.

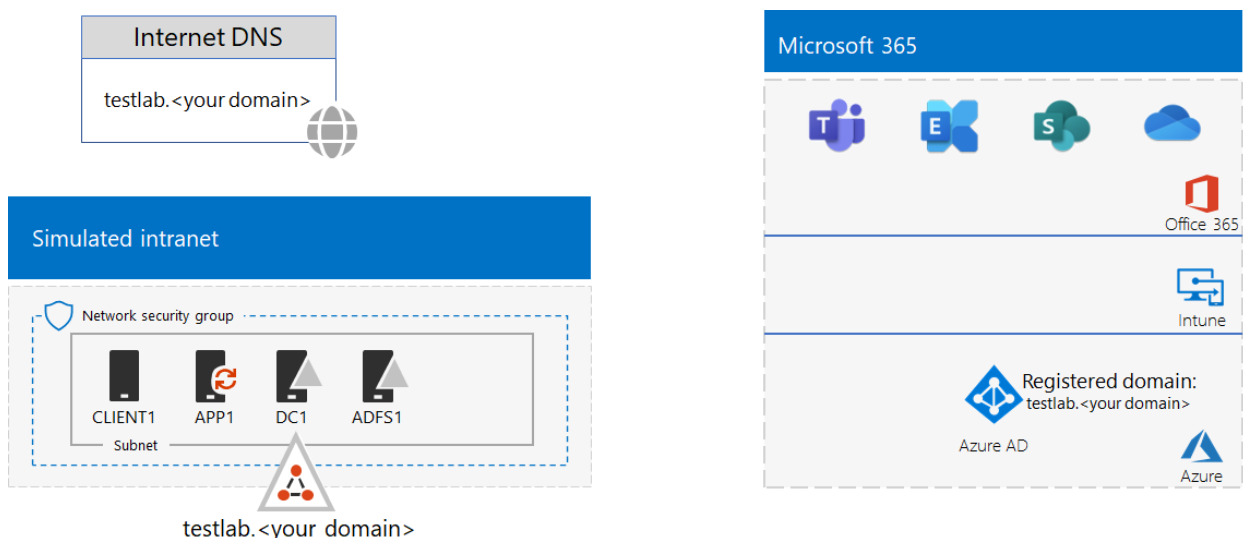
Next, join the ADFS1 virtual machine to the CORP domain with these commands at the Windows PowerShell prompt on ADFS1.

```

$cred=Get-Credential -UserName "CORP\User1" -Message "Type the User1 account password."
Add-Computer -DomainName corp.contoso.com -Credential $cred
Restart-Computer

```

Your resulting configuration looks like this:



Phase 3: Create the web proxy server

PROXY1 provides proxying of authentication messages between users trying to authenticate and ADFS1.

To create an Azure virtual machine for PROXY1, fill in the name of your resource group and Azure location, and then run these commands at the Azure PowerShell command prompt on your local computer.

```
$rgName="<the resource group name of your Base Configuration>"
$vnetName="TlgBaseConfig-01-VNET"
# NOTE: If you built your simulated intranet with Azure PowerShell, comment the previous line with a "#" and
remove the "#" from the next line.
#$vnetName="TestLab"
$staticIP="10.0.0.101"
$locName=(Get-AzResourceGroup -Name $rgName).Location
$vnet=Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $rgName
$pip = New-AzPublicIpAddress -Name PROXY1-PIP -ResourceGroupName $rgName -Location $locName -
AllocationMethod Static
$nic = New-AzNetworkInterface -Name PROXY1-NIC -ResourceGroupName $rgName -Location $locName -SubnetId
$vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
$vm=New-AzVMConfig -VMName PROXY1 -VMSize Standard_D2_v2
$cred=Get-Credential -Message "Type the name and password of the local administrator account for PROXY1."
$vm=Set-AzVMOperatingSystem -VM $vm -Windows -ComputerName PROXY1 -Credential $cred -ProvisionVMAgent -
EnableAutoUpdate
$vm=Set-AzVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-
Datacenter -Version "latest"
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm=Set-AzVMOSDisk -VM $vm -Name "PROXY1-OS" -DiskSizeInGB 128 -CreateOption FromImage -StorageAccountType
"Standard_LRS"
New-AzVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

NOTE

PROXY1 is assigned a static public IP address because you will create a public DNS record that points to it and it must not change when you restart the PROXY1 virtual machine.

Next, add a rule to the network security group for the CorpNet subnet to allow unsolicited inbound traffic from the internet to PROXY1's private IP address and TCP port 443. Run these commands at the Azure PowerShell command prompt on your local computer.

```
$rgName="<the resource group name of your Base Configuration>"
Get-AzNetworkSecurityGroup -Name CorpNet -ResourceGroupName $rgName | Add-AzNetworkSecurityRuleConfig -Name
"HTTPS-to-PROXY1" -Description "Allow TCP 443 to PROXY1" -Access "Allow" -Protocol "Tcp" -Direction
"Inbound" -Priority 101 -SourceAddressPrefix "Internet" -SourcePortRange "*" -DestinationAddressPrefix
"10.0.0.101" -DestinationPortRange "443" | Set-AzNetworkSecurityGroup
```

Next, use the [Azure portal](#) to connect to the PROXY1 virtual machine using the PROXY1 local administrator account name and password, and then open a Windows PowerShell command prompt on PROXY1.

To check name resolution and network communication between PROXY1 and DC1, run the **ping dc1.corp.contoso.com** command and check that there are four replies.

Next, join the PROXY1 virtual machine to the CORP domain with these commands at the Windows PowerShell prompt on PROXY1.

```
$cred=Get-Credential -UserName "CORP\User1" -Message "Type the User1 account password."
Add-Computer -DomainName corp.contoso.com -Credential $cred
Restart-Computer
```

Display the public IP address of PROXY1 with these Azure PowerShell commands on your local computer.

```
Write-Host (Get-AzPublicIpAddress -Name "PROXY1-PIP" -ResourceGroup $rgName).IpAddress
```

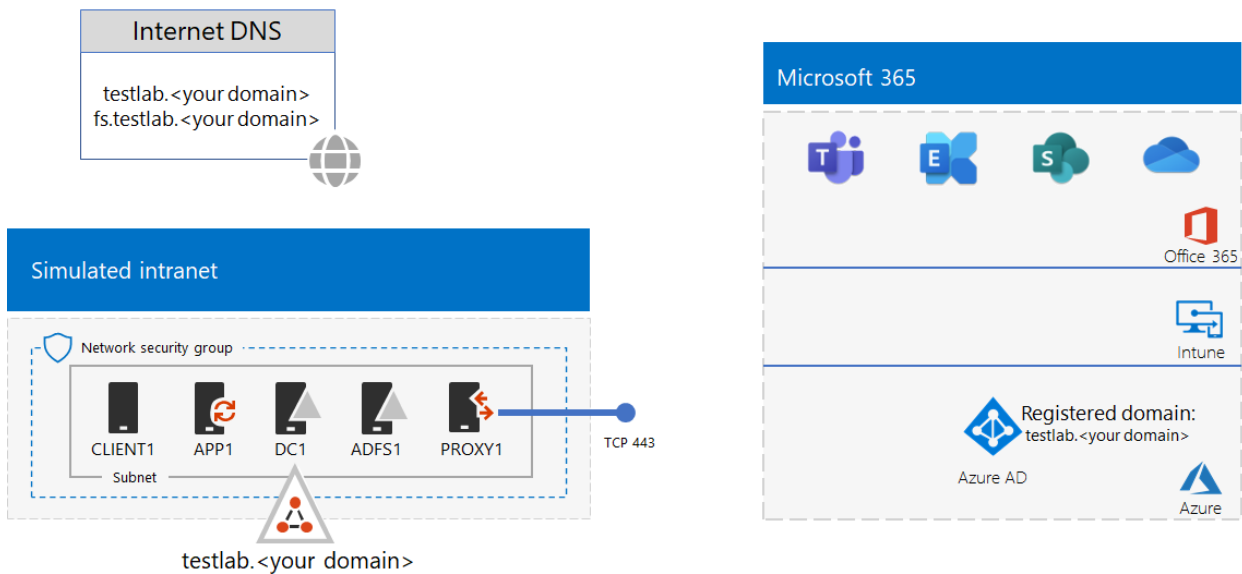
Next, work with your public DNS provider and create a new public DNS A record for **fs.testlab.<your DNS domain name>** that resolves to the IP address displayed by the **Write-Host** command. The **fs.testlab.<your DNS domain name>** is hereafter referred to as the *federation service FQDN*.

Next, use the [Azure portal](#) to connect to the DC1 virtual machine using the CORP\User1 credentials, and then run the following commands at an administrator-level Windows PowerShell command prompt:

```
Add-DnsServerPrimaryZone -Name corp.contoso.com -ZoneFile corp.contoso.com.dns
Add-DnsServerResourceRecordA -Name "fs" -ZoneName corp.contoso.com -AllowUpdateAny -IPv4Address "10.0.0.100"
-TimeToLive 01:00:00
```

These commands create an internal DNS A record so that virtual machines on the Azure virtual network can resolve the internal federation service FQDN to ADFS1's private IP address.

Your resulting configuration looks like this:



Phase 4: Create a self-signed certificate and configure ADFS1 and PROXY1

In this phase, you create a self-signed digital certificate for your federation service FQDN and configure ADFS1 and PROXY1 as an AD FS farm.

First, use the [Azure portal](#) to connect to the DC1 virtual machine using the CORP\User1 credentials, and then open an administrator-level Windows PowerShell command prompt.

Next, create an AD FS service account with this command at the Windows PowerShell command prompt on DC1:

```
New-ADUser -SamAccountName ADFS-Service -AccountPassword (read-host "Set user password" -assecurestring) -
name "ADFS-Service" -enabled $true -PasswordNeverExpires $true -ChangePasswordAtLogon $false
```

Note that this command prompts you to supply the account password. Choose a strong password and record it in a secured location. You will need it for this phase and for Phase 5.

Use the [Azure portal](#) to connect to the ADFS1 virtual machine using the CORP\User1 credentials. Open an administrator-level Windows PowerShell command prompt on ADFS1, fill in your federation service FQDN, and then run these commands to create a self-signed certificate:

```
$fedServiceFQDN="<federation service FQDN>"
New-SelfSignedCertificate -DnsName $fedServiceFQDN -CertStoreLocation "cert:\LocalMachine\My"
New-Item -path c:\Certs -type directory
New-SmbShare -name Certs -path c:\Certs -changeaccess CORP\User1
```

Next, use these steps to save the new self-signed certificate as a file.

1. Select **Start**, enter **mmc.exe**, and then press **Enter**.
2. Select **File > Add/Remove Snap-in**.
3. In **Add or Remove Snap-ins**, double-click **Certificates** in the list of available snap-ins, select **Computer account**, and then select **Next**.
4. In **Select Computer**, select **Finish**, and then select **OK**.
5. In the tree pane, open **Certificates (Local Computer) > Personal > Certificates**.
6. Select and hold (or right-click) the certificate with your federation service FQDN, select **All tasks**, and then select **Export**.
7. On the **Welcome** page, select **Next**.
8. On the **Export Private Key** page, select **Yes**, and then select **Next**.
9. On the **Export File Format** page, select **Export all extended properties**, and then select **Next**.
10. On the **Security** page, select **Password** and enter a password in **Password** and **Confirm password**.
11. On the **File to Export** page, select **Browse**.
12. Browse to the **C:\Certs** folder, enter **SSL** in **File name**, and then select **Save**.
13. On the **File to Export** page, select **Next**.
14. On the **Completing the Certificate Export Wizard** page, select **Finish**. When prompted, select **OK**.

Next, install the AD FS service with this command at the Windows PowerShell command prompt on ADFS1:

```
Install-WindowsFeature ADFS-Federation -IncludeManagementTools
```

Wait for the installation to complete.

Next, configure the AD FS service with these steps:

1. Select **Start**, and then select the **Server Manager** icon.
2. In the tree pane of Server Manager, select **AD FS**.
3. In the tool bar at the top, select the orange caution symbol, and then select **Configure the federation service on this server**.
4. On the **Welcome** page of the Active Directory Federation Services Configuration Wizard, select **Next**.
5. On the **Connect to AD DS** page, select **Next**.
6. On the **Specify Service Properties** page:
 - For **SSL Certificate**, select the down arrow, and then select the certificate with the name of your federation service FQDN.
 - In **Federation Service Display Name**, enter the name of your fictional organization.

- Select **Next**.
7. On the **Specify Service Account** page, select **Select for Account name**.
 8. In **Select User or Service Account**, enter **ADFS-Service**, select **Check Names**, and then select **OK**.
 9. In **Account Password**, enter the password for the ADFS-Service account, and then select **Next**.
 10. On the **Specify Configuration Database** page, select **Next**.
 11. On the **Review Options** page, select **Next**.
 12. On the **Pre-requisite Checks** page, select **Configure**.
 13. On the **Results** page, select **Close**.
 14. Select **Start**, select the power icon, select **Restart**, and then select **Continue**.

From the [Azure portal](#), connect to PROXY1 with the CORP\User1 account credentials.

Next, use these steps to install the self-signed certificate on **both PROXY1 and APP1**.

1. Select **Start**, enter **mmc.exe**, and then press **Enter**.
2. Select **File > Add/Remove Snap-in**.
3. In **Add or Remove Snap-ins**, double-click **Certificates** in the list of available snap-ins, select **Computer account**, and then select **Next**.
4. In **Select Computer**, select **Finish**, and then select **OK**.
5. In the tree pane, open **Certificates (Local Computer) > Personal > Certificates**.
6. Select and hold (or right-click) **Personal**, select **All tasks**, and then select **Import**.
7. On the **Welcome** page, select **Next**.
8. On the **File to Import** page, enter **\\adfs1\certs\ssl.pfx**, and then select **Next**.
9. On the **Private key protection** page, enter the certificate password in **Password**, and then select **Next**.
10. On the **Certificate store** page, select **Next**.
11. On the **Completing** page, select **Finish**.
12. On the **Certificate Store** page, select **Next**.
13. When prompted, select **OK**.
14. In the tree pane, select **Certificates**.
15. Select and hold (or right-click) the certificate, and then select **Copy**.
16. In the tree pane, open **Trusted Root Certification Authorities > Certificates**.
17. Move your mouse pointer below the list of installed certificates, select and hold (or right-click), and then select **Paste**.

Open an administrator-level PowerShell command prompt and run the following command:

```
Install-WindowsFeature Web-Application-Proxy -IncludeManagementTools
```

Wait for the installation to complete.

Use these steps to configure the web application proxy service to use ADFS1 as its federation server:

1. Select **Start**, and then select **Server Manager**.
2. In the tree pane, select **Remote Access**.
3. In the tool bar at the top, select the orange caution symbol, and then select **Open the Web Application Proxy Wizard**.
4. On the **Welcome** page of the Web Application Proxy Configuration Wizard, select **Next**.
5. On the **Federation Server** page:
 - In the **Federation service name** box, enter your federation service FQDN.
 - In the **User name** box, enter **CORP\User1**.
 - In the **Password** box, enter the password for the User1 account.
 - Select **Next**.
6. On the **AD FS Proxy Certificate** page, select the down arrow, select the certificate with your federation service FQDN, and then select **Next**.
7. On the **Confirmation** page, select **Configure**.
8. On the **Results** page, select **Close**.

Phase 5: Configure Microsoft 365 for federated identity

Use the [Azure portal](#) to connect to the APP1 virtual machine with the CORP\User1 account credentials.

Use these steps to configure Azure AD Connect and your Microsoft 365 subscription for federated authentication:

1. From the desktop, double-click **Azure AD Connect**.
2. On the **Welcome to Azure AD Connect** page, select **Configure**.
3. On the **Additional tasks** page, select **Change user sign-in**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter your global administrator account name and password, and then select **Next**.
5. On the **User sign-in** page, select **Federation with AD FS**, and then select **Next**.
6. On the **AD FS farm** page, select **Use an existing AD FS farm**, enter **ADFS1** in the **Server Name** box, and then select **Next**.
7. When prompted for server credentials, enter the credentials of the CORP\User1 account, and then select **OK**.
8. On the **Domain Administrator** credentials page, enter **CORP\User1** in the **Username** box, enter the account password in the **Password** box, and then select **Next**.
9. On the **AD FS service account** page, enter **CORP\ADFS-Service** in the **Domain Username** box, enter the account password in the **Domain User Password** box, and then select **Next**.
10. On the **Azure AD Domain** page, in **Domain**, select the name of the domain that you previously created and added to your subscription in Phase 1, and then select **Next**.
11. On the **Ready to configure** page, select **Configure**.

12. On the **Installation complete** page, select **Verify**.

You should see messages indicating that both the intranet and internet configuration was verified.

13. On the **Installation complete** page, select **Exit**.

To demonstrate that federated authentication is working:

1. Open a new private instance of your browser on your local computer and go to

<https://admin.microsoft.com>.

2. For the sign-in credentials, enter **user1@** <the domain created in Phase 1>.

For example, if your test domain is **testlab.contoso.com**, you would enter "user1@testlab.contoso.com". Press the **Tab** key or allow Microsoft 365 to automatically redirect you.

You should now see a **Your connection is not private** page. You are seeing this because you installed a self-signed certificate on ADFS1 that your desktop computer can't validate. In a production deployment of federated authentication, you would use a certificate from a trusted certification authority and your users would not see this page.

3. On the **Your connection is not private** page, select **Advanced**, and then select **Proceed to <your federation service FQDN>**.

4. On the page with the name of your fictional organization, sign in with the following:

- **CORP\User1** for the name
- The password for the User1 account

You should see the **Microsoft Office Home** page.

This procedure demonstrates that your trial subscription is federated with the AD DS corp.contoso.com domain hosted on DC1. Here are the basics of the authentication process:

1. When you use the federated domain that you created in Phase 1 within the sign-in account name, Microsoft 365 redirects your browser to your federation service FQDN and PROXY1.
2. PROXY1 sends your local computer the fictional company sign-in page.
3. When you send CORP\User1 and the password to PROXY1, it forwards them to ADFS1.
4. ADFS1 validates CORP\User1 and the password with DC1 and sends your local computer a security token.
5. Your local computer sends the security token to Microsoft 365.
6. Microsoft 365 validates that the security token was created by ADFS1 and allows access.

Your trial subscription is now configured with federated authentication. You can use this dev/test environment for advanced authentication scenarios.

Next step

When you are ready to deploy production-ready, high availability federated authentication for Microsoft 365 in Azure, see [Deploy high availability federated authentication for Microsoft 365 in Azure](#).

Azure AD Seamless Single Sign-on for your Microsoft 365 test environment

10/28/2022 • 3 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

Azure AD Seamless Single Sign-On (Seamless SSO) automatically signs in users when they are on their PCs or devices that are connected to their organization network. Azure AD Seamless SSO provides users with easy access to cloud-based applications without needing any additional on-premises components.

This article describes how to configure your Microsoft 365 test environment for Azure AD Seamless SSO.

Setting up Azure AD Seamless SSO involves two phases:

- [Phase 1: Configure password hash synchronization for your Microsoft 365 test environment](#)
- [Phase 2: Configure Azure AD Connect on APP1 for Azure AD Seamless SSO](#)



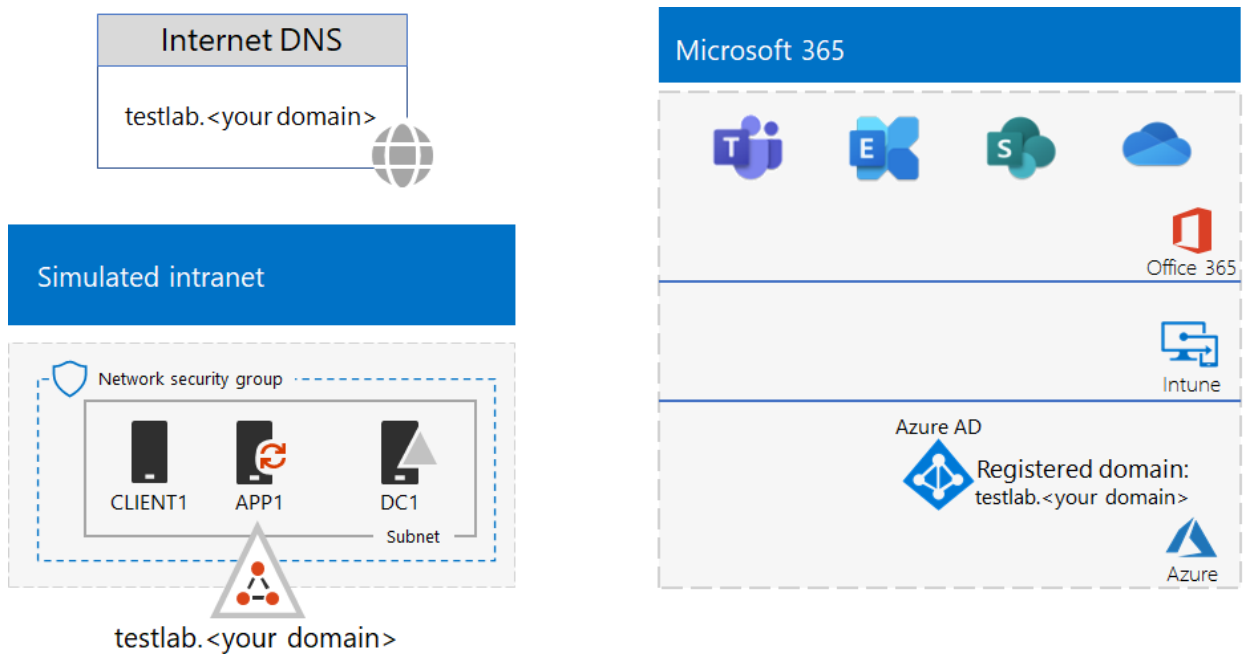
TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

Follow the instructions in [password hash synchronization for Microsoft 365](#).

Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscription.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to periodically synchronize the TESTLAB Active Directory Domain Services (AD DS) domain to the Azure AD tenant of your Microsoft 365 subscription.

Phase 2: Configure Azure AD Connect on APP1 for Azure AD Seamless SSO

In this phase, configure Azure AD Connect on APP1 for Azure AD Seamless SSO, and then verify that it works.

Configure Azure AD Connect on APP1

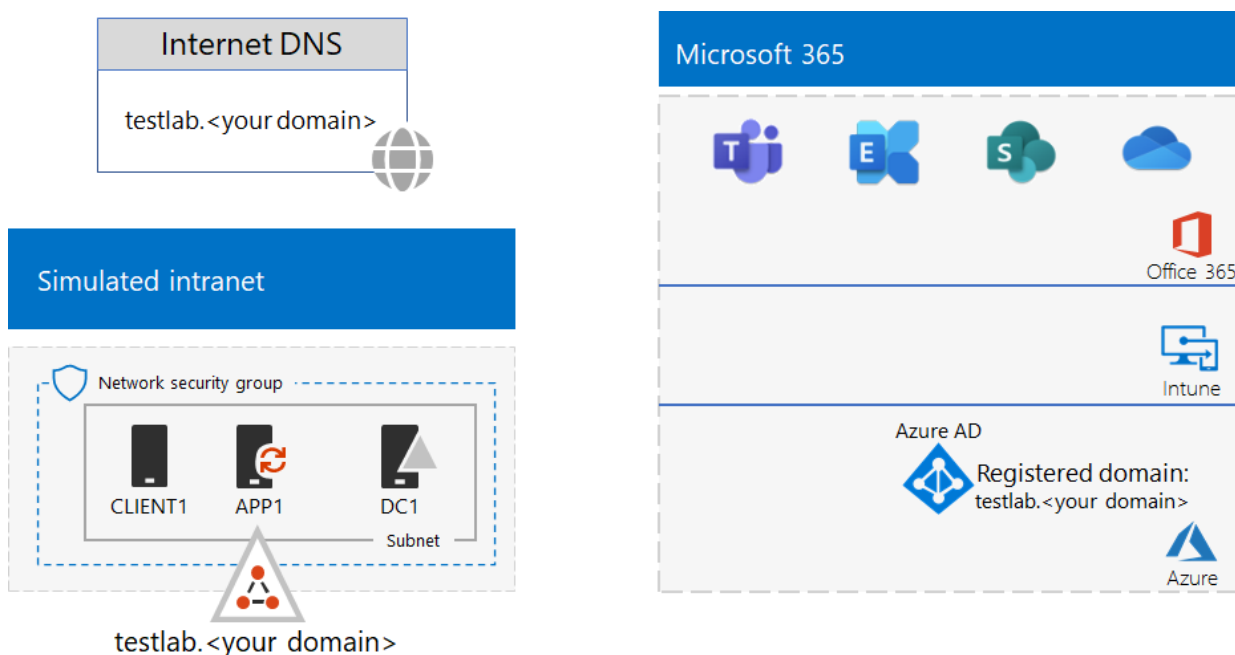
1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the APP1 desktop, run Azure AD Connect.
3. On the **Welcome page**, select **Configure**.
4. On the **Additional tasks** page, select **Change user sign-in**, and then select **Next**.
5. On the **Connect to Azure AD** page, enter your global administrator account credentials, and then select **Next**.
6. On the **User sign-in** page, select **Enable single sign-on**, and then select **Next**.
7. On the **Enable single sign-on** page, select **Enter credentials**.
8. In the **Windows Security** dialog box, enter **user1** and the password of the user1 account, select **OK**, and then select **Next**.
9. On the **Ready to Configure** page, select **Configure**.
10. On the **Configuration complete** page, select **Exit**.
11. From the Azure portal, in the left pane, select **Azure Active Directory** > **Azure AD Connect**. Verify that the **Seamless single sign-on** feature appears as **Enabled**.

Next, test the ability to sign in to your subscription with the **user1@testlab.<your public domain>** user name of the User1 account.

1. From Internet Explorer on APP1, select the settings icon, and then select **Internet Options**.
2. In **Internet Options**, select the **Security** tab.
3. Select **Local intranet**, and then select **Sites**.
4. In **Local intranet**, select **Advanced**.
5. In **Add this website to the zone**, enter **https://autologon.microsoftazuread-sso.com**, select **Add** > **Close** > **OK** > **OK**.
6. Sign out, and then sign in again, this time specifying a different account.
7. When prompted to sign in, specify **user1@testlab.<your public domain>** name, and then select **Next**.
You should successfully sign in as User1 without being prompted for a password. This proves that Azure AD Seamless SSO is working.

Notice that although User1 has domain administrator permissions for the TESTLAB AD DS domain, it is not a global administrator for Azure AD. Therefore, you will not see the **Admin** icon as an option.

Here is your resulting configuration:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscriptions with the DNS domain `testlab.<your domain name>` registered.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the list of accounts and groups from the Azure AD tenant of your Microsoft 365 subscription to the TESTLAB AD DS domain.
- Azure AD Seamless SSO is enabled so that computers on the simulated intranet can sign in to Microsoft 365 cloud resources without specifying a user account password.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Multi-factor authentication for your Microsoft 365 for enterprise test environment

10/28/2022 • 5 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

For an additional level of security for signing in to Microsoft 365 or any service or application that uses the Azure AD tenant for your subscription, you can enable Azure AD multi-factor authentication, which requires more than just a username and password to verify an account.

With multi-factor authentication, users are required to acknowledge a phone call, type a verification code sent in a text message, or verify the authentication with an app on their smart phones after correctly entering their passwords. They can sign in only after this second authentication factor is satisfied.

This article describes how to enable and test text message-based authentication for a specific user account.

Setting up multi-factor authentication for an account in your Microsoft 365 for enterprise test environment involves two phases and a third optional phase:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Enable and test multi-factor authentication for the User 2 account](#)
- [Phase 3: Enable and test multi-factor authentication with a conditional access policy](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you just want to test multi-factor authentication in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test multi-factor authentication in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing multi-factor authentication does not require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It is provided here as an option so that you can test multi-factor authentication and experiment with it in an environment that represents a typical organization.

Phase 2: Enable and test multi-factor authentication for the User 2 account

Enable multi-factor authentication for the User 2 account with these steps:

1. Open a separate, private instance of your browser, go to the Microsoft 365 admin center (<https://portal.microsoft.com>), and then sign in with your global administrator account.
2. In the left navigation, select **Users** > **Active users**.
3. In the Active users pane, select **Multi-factor authentication**.
4. In the list, select the **User 2** account.
5. In the **User 2** section, under **Quick steps**, select **Enable**.
6. In the **About enabling multi-factor auth** dialog box, select **Enable multi-factor auth**.
7. In the **Updates successful** dialog box, select **Close**.
8. On the **Microsoft 365 admin center** tab, select the user account icon in the upper right, and then select **Sign out**.
9. Close your browser instance.

Complete the configuration for the User 2 account to use a text message for validation and test it with these steps:

1. Open a new, private instance of your browser.
2. Go to the [Microsoft 365 admin center](#) and sign in with the User 2 account name and password.
3. After signing in, you are prompted to set up the account for more information. Select **Next**.
4. On the **Additional security verification** page:
 - Select your country or region.
 - Enter the phone number of the smart phone that will receive text messages.
 - In **Method**, select **Send me a code by text message**.
5. Select **Next**.
6. Enter the verification code from the text message received on your smart phone, and then select **Verify**.
7. On the **Step 3: Keep your existing applications** page, select **Done**.
8. If this is the first time you signed in with the User 2 account, you are prompted to change the password. Enter the original password and a new password twice, and then select **Update password and sign in**. Record the new password in a secure location.

You should see the Office portal for User 2 on the **Microsoft Office Home** tab of your browser.

Phase 3: Enable and test multi-factor authentication with a conditional access policy

This phase can only be used for a Microsoft 365 for enterprise test environment.

In this phase, you enable multi-factor authentication for the User 3 account using a group and a conditional access policy.

Next, create a new group named MFAUsers and add the User 3 account to it.

1. On the **Microsoft 365 admin center** tab, select **Groups** in the left navigation, and then select **Groups**.
2. Select **Add a group**.
3. In the **Choose a group type** pane, select **Security**, and then select **Next**.
4. In the **Set up the basics** pane, select **Create group**, and then select **Close**.
5. In the **Review and finish adding group** pane, enter **MFAUsers**, and then select **Next**.
6. In the list of groups, select the **MFAUsers** group.
7. In the **MFAUsers** pane, select **Members**, and then select **View all and manage members**.
8. In the **MFAUsers** pane, select **Add members**, select the **User 3** account, and then select **Save > Close > Close**.

Next, create a conditional access policy to require multifactor authentication for members of the MFAUsers group.

1. In a new tab of your browser, go to <https://portal.azure.com>.
2. Select **Azure Active Directory > Security > Conditional Access**.
3. In the **Conditional access – Policies** pane, select **New policy**.
4. In the **New** pane, enter **MFA for user accounts** in the **Name** box.
5. In the **Assignments** section, select **Users and groups**.
6. On the **Include** tab of the **Users and groups** pane, select **Select users and groups > Users and groups > Select**.
7. In the **Select** pane, select the **MFAUsers** group, and then select **Select > Done**.
8. In the **Access controls** section of the **New** pane, select **Grant**.
9. In the **Grant** pane, select **Require multi-factor authentication**, and then select **Select**.
10. In the **New** pane, select **On** for **Enable policy**, and then select **Create**.
11. Close the **Azure portal** and **Microsoft 365 admin center** tabs.

To test this policy, sign out and sign in with the User 3 account. You should be prompted to configure MFA. This demonstrates that the MFAUsers policy is being applied.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Protect global administrator accounts in your Microsoft 365 for enterprise test environment

10/28/2022 • 3 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

You can prevent digital attacks on your organization by ensuring that your administrator accounts are as secure as possible.

This article describes how to use Azure Active Directory (Azure AD) conditional access policies to protect global administrator accounts.

Protecting global administrator accounts in your Microsoft 365 for enterprise test environment involves two phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Configure conditional access policies](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you want to test global administrator account protection in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test global administrator account protection in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing global administrator account protection does not require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services (AD DS). It is provided here as an option so that you can test global administrator account protection and experiment with it in an environment that represents a typical organization.

Phase 2: Configure conditional access policies

First, create a new user account as a dedicated global administrator.

1. On a separate tab, open the [Microsoft 365 admin center](#).
2. Select **Users > Active users**, and then select **Add a user**.
3. In the **Add user** pane, enter **DedicatedAdmin** in the **First name**, **Display name**, and **Username** boxes.

4. Select **Password**, select **Let me create the password**, and then enter a strong password. Record the password for this new account in a secure location.
5. Select **Next**.
6. In the **Assign product licenses** pane, select **Microsoft 365 E5**, and then select **Next**.
7. In the **Optional settings** pane, select **Roles > Admin center access > Global admin > Next**.
8. On the **You're almost done** pane, select **Finish adding**, and then select **Close**.

Next, create a new group named GlobalAdmins and add the DedicatedAdmin account to it.

1. On the **Microsoft 365 admin center** tab, select **Groups** in the left navigation, and then select **Groups**.
2. Select **Add a group**.
3. In the **Choose a group type** pane, select **Security**, and then select **Next**.
4. In the **Set up the basics** pane, select **Create group**, and then select **Close**.
5. In the **Review and finish adding group** pane, enter **GlobalAdmins**, and then select **Next**.
6. In the list of groups, select the **GlobalAdmins** group.
7. In the **GlobalAdmins** pane, select **Members**, and then select **View all and manage members**.
8. In the **GlobalAdmins** pane, select **Add members**, select the **DedicatedAdmin** account and your global admin account, and then select **Save > Close > Close**.

Next, create conditional access policies to require multi-factor authentication for global administrator accounts and to deny authentication if the sign-in risk is medium or high.

This first policy requires that all global administrator accounts use MFA.

1. In a new tab of your browser, go to <https://portal.azure.com>.
2. Click **Azure Active Directory > Security > Conditional Access**.
3. In the **Conditional access – Policies** pane, select **Baseline policy: Require MFA for admins (preview)**.
4. In the **Baseline policy** pane, select **Use policy immediately > Save**.

This second policy blocks access to global administrator account authentication when the sign-in risk is medium or high.

1. In the **Conditional access – Policies** pane, select **New policy**.
2. In the **New** pane, enter **Global administrators** in **Name**.
3. In the **Assignments** section, select **Users and groups**.
4. On the **Include** tab of the **Users and groups** pane, select **Select users and groups > Users and groups > Select**.
5. In the **Select** pane, select the **GlobalAdmins** group, and then select **Select > Done**.
6. In the **Assignments** section, select **Conditions**.
7. In the **Conditions** pane, select **Sign-in risk**, select **Yes** for **Configure**, select **High** and **Medium**, and then select **Select and Done**.
8. In the **Access controls** section of the **New** pane, select **Grant**.
9. In the **Grant** pane, select **Block access**, and then select **Select**.
10. In the **New** pane, select **On** for **Enable policy**, and then select **Create**.
11. Close the **Azure portal** and **Microsoft 365 admin center** tabs.

To test the first policy, sign out and sign in with the DedicatedAdmin account. You should be prompted to configure MFA. This demonstrates that the first policy is being applied.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Password writeback for your Microsoft 365 test environment

10/28/2022 • 3 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

Users can use password writeback to update their passwords through Azure Active Directory (Azure AD), which is then replicated to your local Active Directory Domain Services (AD DS). With password writeback, users don't have to update their passwords through the on-premises AD DS where their original user accounts are stored. This helps roaming or remote users who don't have a remote access connection to their on-premises network.

This article describes how to configure your Microsoft 365 test environment for password writeback.

Configuring your test environment for password writeback involves two phases:

- [Phase 1: Configure password hash synchronization for your Microsoft 365 test environment](#)
- [Phase 2: Enable password writeback for the TESTLAB AD DS domain](#)

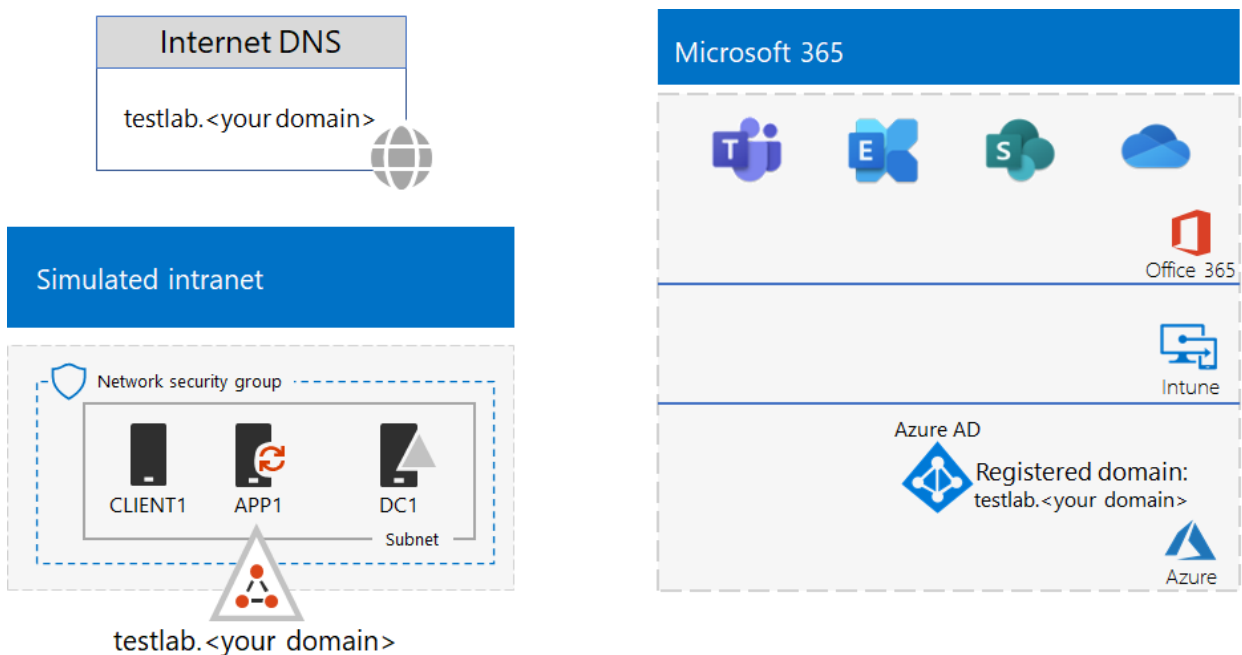


TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

First, follow the instructions in [password hash synchronization](#). Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscription.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the TESTLAB AD DS domain to the Azure AD tenant of your Microsoft 365 subscription.

Phase 2: Enable password writeback for the TESTLAB AD DS domain

First, configure the User 1 account with the global administrator role.

1. From the [Microsoft 365 admin center](#), sign in with your global administrator account.
2. Select **Active users**.
3. On the **Active users** page, select the **user1** account,
4. On the **user1** pane, select **Edit** next to **Roles**.
5. On the **Edit user roles** pane for user1, select **Global administrator**, select **Save**, and then select **Close**.

Next, configure the User 1 account with the security settings that allow it to change passwords on behalf of other users in the TESTLAB AD DS domain.

1. From the [Azure portal](#), sign in with your global administrator account, and then connect to APP1 with the TESTLAB\User1 account.
2. From the desktop of APP1, select **Start**, enter **active**, and then select **Active Directory Users and Computers**.
3. On the menu bar, select **View**. If **Advanced features** is not enabled, select it to enable it.
4. In the tree pane, select and hold (or right-click) your domain, select **Properties**, and then select the **Security** tab.
5. Select **Advanced**.
6. On the **Permissions** tab, select **Add**.
7. Select **Select a principal**, enter **User1**, and then select **OK**.
8. In **Applies to**, select **Descendant User objects**.
9. Under **Permissions**, select the following:
 - **Change password**
 - **Reset password**
10. Under **Properties**, select the following:
 - **Write lockoutTime**
 - **Write pwdLastSet**
11. Select **OK** three times to save the changes.
12. Close **Active Directory Users and Computers**.

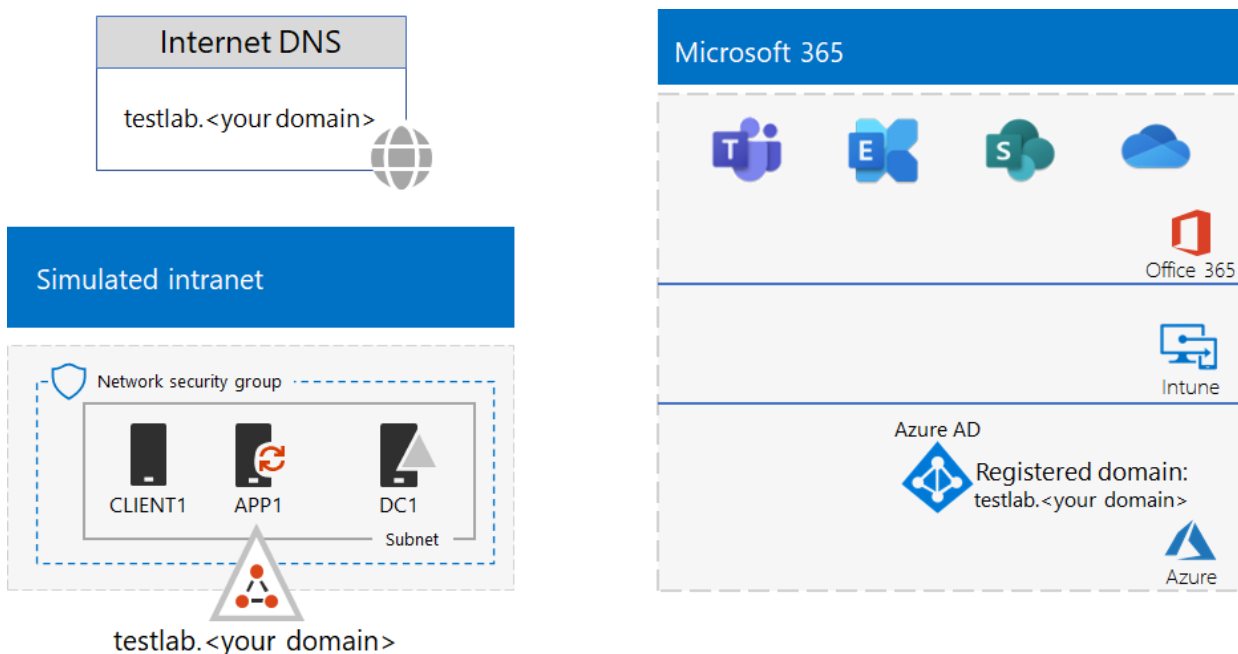
Next, configure Azure AD Connect on APP1 for password writeback.

1. If needed, connect to APP1 with the TESTLAB\User1 account.

2. From the desktop of APP1, double-click **Azure AD Connect**.
3. On the **Welcome page**, select **Configure**.
4. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
5. On the **Connect to Azure AD** page, enter your global administrator account credentials, and then select **Next**.
6. On the **Connect directories** and **Domain/OU filtering** pages, select **Next**.
7. On the **Optional features** page, select **Password writeback**, and then select **Next**.
8. On the **Ready to configure** page, select **Configure** and wait for the process to finish.
9. When you see the configuration finish, select **Exit**.

You are now ready to test password writeback for users on computers that aren't connected to the virtual network of your simulated intranet.

Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscriptions with the DNS domain TESTLAB.<your domain name> registered.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the list of accounts and groups from the Azure AD tenant of your Microsoft 365 subscription to the TESTLAB AD DS domain.
- Password writeback is enabled so that users can change their passwords through Azure AD without having to be connected to the simplified intranet.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Password reset for your Microsoft 365 test environment

10/28/2022 • 3 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

Azure Active Directory (Azure AD) self-service password reset (SSPR) allows users to reset or unlock their passwords or accounts.

This article describes how to configure and test password resets in your Microsoft 365 test environment.

Setting up SSPR involves three phases:

- [Phase 1: Configure password hash synchronization for your Microsoft 365 test environment](#)
- [Phase 2: Enable password writeback](#)
- [Phase 3: Configure and test password reset](#)



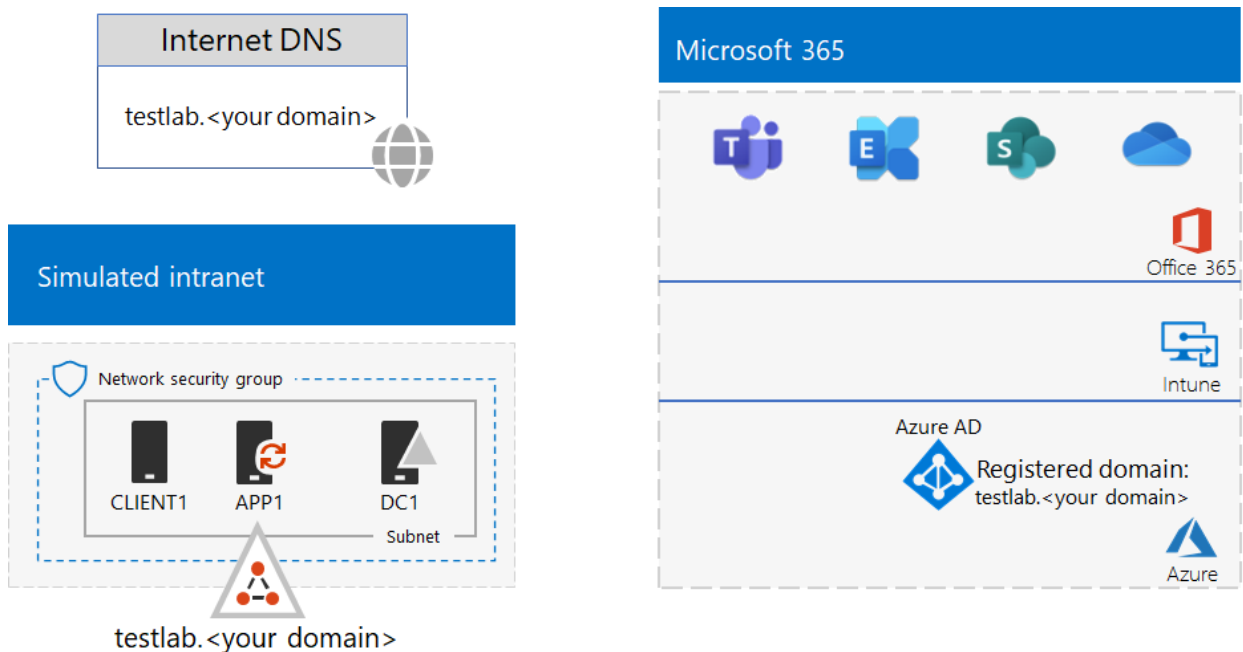
TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Configure password hash synchronization for your Microsoft 365 test environment

First, follow the instructions in [password hash synchronization](#).

Your resulting configuration looks like this:



This configuration consists of:

- A Microsoft 365 E5 trial or paid subscription.
- A simplified organization intranet connected to the internet, consisting of the DC1, APP1, and CLIENT1 virtual machines on a subnet of an Azure virtual network.
- Azure AD Connect runs on APP1 to synchronize the TESTLAB Active Directory Domain Services (AD DS) domain to the Azure AD tenant of your Microsoft 365 subscription.

Phase 2: Enable password writeback

Follow the instructions in [Phase 2 of the password writeback Test Lab Guide](#).

You must have password writeback enabled to use password reset.

Phase 3: Configure and test password reset

In this phase, configure password reset in the Azure AD tenant through group membership, and then verify that it works.

First, enable password reset for the accounts in a specific Azure AD group.

1. From a private instance of your browser, open <https://portal.azure.com>, and then sign in with the credentials of your global administrator account.
2. In the Azure portal, select **Azure Active Directory** > **Groups** > **New group**.
3. Set the **Group type** to **Security**, **Group name** to **PWReset**, and the **Membership type** to **Assigned**.
4. Select **Members**, find and select **User 3**, select **Select**, and then select **Create**.
5. Close the **Groups** pane.
6. In the Azure Active Directory pane, select **Password reset** in the left navigation.
7. In the **Password reset-Properties** pane, under the option **Self Service Password Reset Enabled**, choose **Selected**.
8. Select **Select group**, select the **PWReset** group, and then select **Select** > **Save**.
9. Close the private browser instance.

Next, test password reset for the User 3 account.

1. Open a new private browser instance and browse to <https://aka.ms/ssprsetup>.

2. Sign in with the User 3 account credentials.
3. In **More information required**, select **Next**.
4. In **Don't lose access to your account**, set the authentication phone to your mobile phone number and the authentication email to your work or personal email account.
5. After both are verified, select **Looks good**, and then close the private instance of the browser.
6. In a new private browser instance, go to <https://aka.ms/sspr>.
7. Enter the User 3 account name, enter the characters from the CAPTCHA, and then select **Next**.
8. For **verification step 1**, select **Email my alternate email**, and then select **Email**. When you receive the email, enter the verification code, and then select **Next**.
9. In **Get back into your account**, enter a new password for the User 3 account, and then select **Finish**. Note the changed password of the User 3 account and store it in a safe location.
10. In a separate tab of the same browser, go to <https://admin.microsoft.com>, and then sign in with the User 3 account name and its new password. You should see the **Microsoft Office Home** page.

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Automate licensing and group membership for your Microsoft 365 for enterprise test environment

10/28/2022 • 3 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

Group-based licensing automatically assigns or removes licenses for a user account based on group membership. Dynamic group membership adds or removes members to a group based on user account properties, such as **Department** or **Country**. This article steps you through demonstrations of both adding and removing group members in your Microsoft 365 for enterprise test environment.

Setting up auto-licensing and dynamic group membership in your Microsoft 365 for enterprise test environment involves two phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Configure and test dynamic group membership and automatic licensing](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you want to only test automated licensing and group membership in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test automated licensing and group membership in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing automated licensing and group membership doesn't require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It's provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Configure and test dynamic group membership and automatic licensing

First, create a new group named Sales, and add a dynamic group membership rule so that user accounts with the **Department** set to **Sales** automatically join the Sales group.

1. In a private instance of your internet browser, sign in to the [Microsoft 365 admin center](#) with the global

administrator account of your Microsoft 365 E5 test lab subscription.

2. On a separate tab of your browser, go to the Azure portal at <https://portal.azure.com>.
3. In the Azure portal, enter **groups** in the search box, and then select **Groups**.
4. In the **All groups** pane, select **New group**.
5. In **Group type**, select **Microsoft 365**.
6. In **Group name**, enter **Sales**.
7. In **Membership type**, select **Dynamic user**.
8. Select **Dynamic user members**.
9. In the **Dynamic membership rules** pane:
 - Select the **department** property.
 - Select the **Equals** operator.
 - In the **Value** box, enter **Sales**.
10. Select **Save**.
11. Select **Create**.

Next, configure the Sales group so that members are automatically assigned the Microsoft 365 E5 license.

1. Select the **Sales** group, and then select **Licenses**.
2. In the **Update license assignments** pane, select **Microsoft 365 E5**, and then select **Save**.
3. In your browser, close the Azure portal tab.

Next, test dynamic group membership and automatic licensing on the User 4 account:

1. From the **Microsoft Office Home** tab in your browser, select **Admin**.
2. From the **Microsoft 365 admin center** tab, select **Active users**.
3. On the **Active users** page, select the **User 4** account.
4. On the **User 4** pane, select **Edit** for **Product licenses**.
5. On the **Product licenses** pane, disable the **Microsoft 365 E5** license, and then select **Save > Close**.
6. In the properties of the User 4 account, verify that no product licenses have been assigned and there are no group memberships.
7. For **Contact information**, select **Edit**.
8. In the **Edit Contact information** pane, select **Contact information**.
9. In the **Department** box, enter **Sales**, and then select **Save > Close**.
10. Wait a few minutes, and then periodically select the **Refresh** icon in the upper-right of the User 4 account pane.

In time, you should see the:

- **Group memberships** property updated with the **Sales** group.
- **Product licenses** property updated with the **Microsoft 365 E5** license.

See these articles to deploy dynamic group membership and automatic licensing in production:

- [Group-based licensing in Azure Active Directory](#)
- [Dynamic groups in Azure Active Directory](#)

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Azure AD Identity Protection for your Microsoft 365 for enterprise test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

You can use Azure Active Directory (Azure AD) Identity Protection to detect potential vulnerabilities that affect your organization's identities, configure automated responses, and investigate incidents. This article describes how to use Azure AD Identity Protection to view the analysis of your test environment accounts.

Setting up Azure AD Identity Protection in your Microsoft 365 for enterprise test environment involves two phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Use Azure AD Identity Protection](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you want to only test Azure AD Identity Protection in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to test Azure AD Identity Protection in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing Azure AD Identity Protection doesn't require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It is provided here as an option so that you can test Azure AD Identity Protection and experiment with it in an environment that represents a typical organization.

Phase 2: Use Azure AD Identity Protection

1. Open a private instance of your browser and sign in to the Azure portal at <https://portal.azure.com> with the global administrator account of your Microsoft 365 for enterprise test environment.
2. In the Azure portal, type **identity protection** in the search box, and then select **Azure AD Identity Protection**.
3. In the **Identity Protection - Overview** blade, select each report to see what it's reporting.
4. Under **Notify**, select **Users at risk detected alerts**.

5. In the **Users at risk detected alerts** pane, select **Medium**.
6. For **Emails are sent to the following users**, select **Included** and verify that your global admin account is in the list of selected members.
7. Select **Save**.

Under **Protect**, select various policies to see how to configure them. If you create and activate a policy, make sure that it's not blocking access for all users, or you might not be able to sign in. To prevent this, exclude specific user accounts, such as global admins.

For further testing and experimentation, see [Simulating risk events](#).

Next step

Explore additional [identity](#) features and capabilities in your test environment.

See also

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Identity and device access for your Microsoft 365 test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

[Identity and device access configurations](#) are a set of recommended configurations and conditional access policies to protect access to all services that are integrated with Azure Active Directory (Azure AD).

To create a test environment that has the common identity and device access configurations in place:

1. Configure your test environment with the prerequisite identity and security features based on your choice of identity model and authentication method:
 - [Cloud only](#)
 - [Password hash synchronization \(PHS\)](#)
 - [Pass-through authentication \(PTA\)](#)
2. Use [Common identity and device access policies](#) to configure the policies that build on the prerequisites configured for your test environment and explore and verify protection for identities and devices.

See also

[Additional identity Test Lab Guides](#)

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Identity and device access prerequisites for cloud only in your Microsoft 365 test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

[Identity and device access configurations](#) are a set of recommended configurations and conditional access policies to protect access to all services that are integrated with Azure Active Directory (Azure AD).

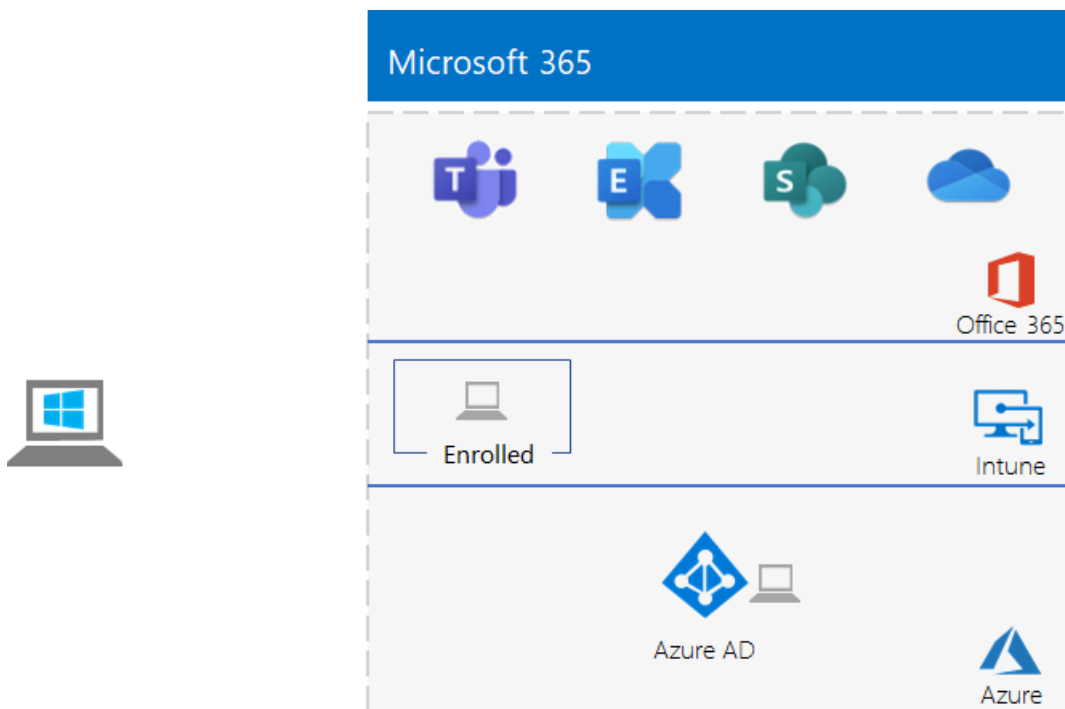
This article describes how to configure a Microsoft 365 test environment that meets the requirements of the [cloud only prerequisite configuration](#) for identity and device access.

There are eight phases to setting up this test environment:

1. Build out your lightweight test environment
2. Configure named locations
3. Configure self-service password reset
4. Configure multifactor authentication
5. Enable automatic device registration of domain-joined Windows computers
6. Configure Azure AD password protection
7. Enable Azure AD Identity Protection
8. Enable modern authentication for Exchange Online and Skype for Business Online

Phase 1: Build out your lightweight Microsoft 365 test environment

Follow the instructions in [Lightweight base configuration](#). Here is the resulting configuration.



Phase 2: Configure named locations

First, determine the public IP addresses or address ranges used by your organization.

Next, follow the instructions in [Configure named locations in Azure Active Directory](#) to add the addresses or address ranges as named locations.

Phase 3: Configure self-service password reset

Follow the instructions in [Phase 3 of the password reset Test Lab Guide](#).

When enabling password reset for the accounts in a specific Azure AD group, add these accounts to the **Password reset** group:

- User 2
- User 3
- User 4
- User 5

Test password reset only for the User 2 account.

Phase 4: Configure multi-factor authentication

Follow the instructions in [Phase 2 of the multi-factor authentication Test Lab Guide](#) for the following user accounts:

- User 2
- User 3
- User 4
- User 5

Test multi-factor authentication only for the User 2 account.

Phase 5: Enable automatic device registration of domain-joined Windows computers

Follow [these instructions](#) to enable automatic device registration of domain-joined Windows computers.

Phase 6: Configure Azure AD password protection

Follow [these instructions](#) to block known weak passwords and their variants.

Phase 7: Enable Azure AD Identity Protection

Follow the instructions in [Phase 2 of the Azure AD Identity Protection Test Lab Guide](#).

Phase 8: Enable modern authentication for Exchange Online and Skype for Business Online

For Exchange Online, follow [these instructions](#).

For Skype for Business Online:

1. Connect to [Skype for Business Online](#).
2. Run this command.

```
Set-CsOauthConfiguration -ClientAdalAuthOverride Allowed
```

3. Verify that the change was successful with this command.

```
Get-CsOauthConfiguration
```

The result is a test environment that meets the requirements of the [cloud-only prerequisite configuration](#) for identity and device access.

Next step

Use [Common identity and device access policies](#) to configure the policies that build on the prerequisites and protect identities and devices.

See also

[Additional identity Test Lab Guides](#)

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Identity and device access prerequisites for password hash synchronization in your Microsoft 365 test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

[Identity and device access configurations](#) are a set of configurations and conditional access policies to protect access to all services in Microsoft 365 for enterprise that are integrated with Azure Active Directory (Azure AD).

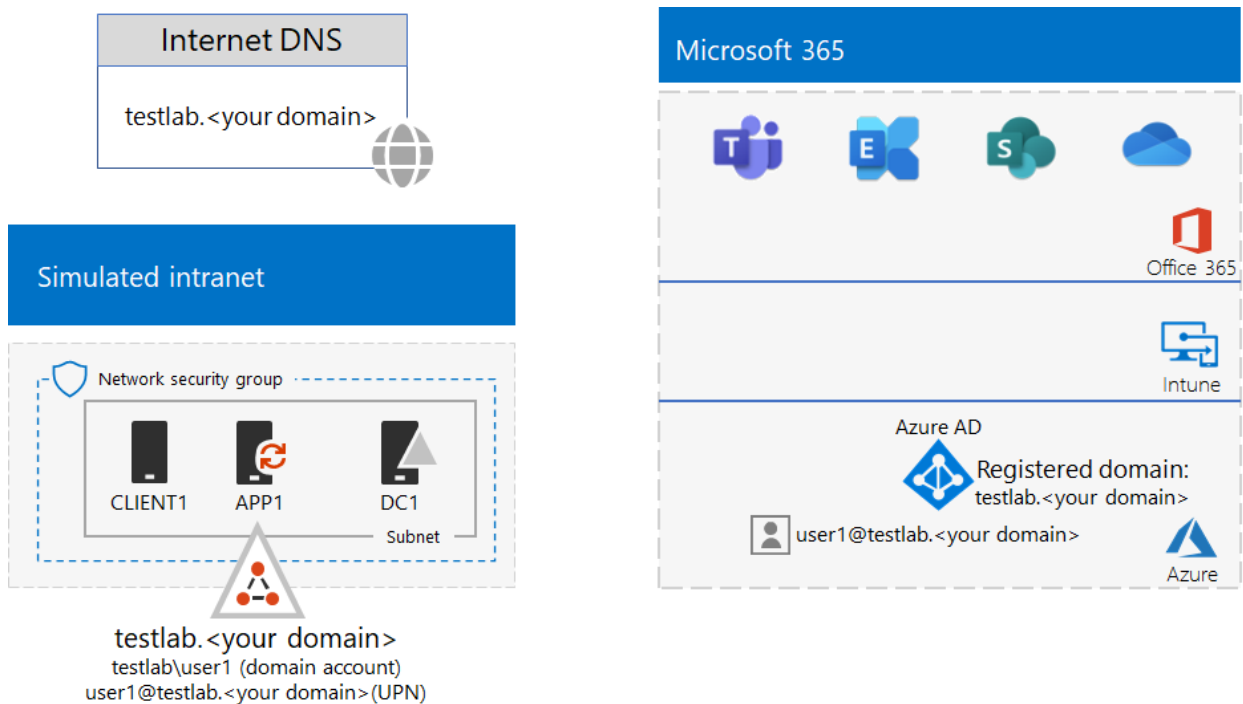
This article describes how to configure a Microsoft 365 test environment that meets the requirements of the [hybrid with password hash sync authentication prerequisite configuration](#) for identity and device access.

There are ten phases to setting up this test environment:

1. Create a simulated enterprise with password hash sync test environment
2. Configure Azure AD seamless single sign-on
3. Configure named locations
4. Configure password writeback
5. Configure self-service password reset for all user accounts
6. Configure multifactor authentication for all user accounts
7. Enable automatic device registration of domain-joined Windows computers
8. Configure Azure AD password protection
9. Enable Azure AD Identity Protection
10. Enable modern authentication for Exchange Online and Skype for Business Online

Phase 1: Build out your simulated enterprise with password hash sync Microsoft 365 test environment

Follow the instructions in [the password hash synchronization](#) Test Lab Guide. Here is the resulting configuration.



Phase 2: Configure Azure AD seamless single sign-on

Follow the instructions in [Phase 2 of the Azure AD Seamless Single Sign-on Test Lab Guide](#).

Phase 3: Configure named locations

First, determine the public IP addresses or address ranges used by your organization.

Next, follow the instructions in [Configure named locations in Azure Active Directory](#) to add the addresses or address ranges as named locations.

Phase 4: Configure password writeback

Follow the instructions in [Phase 2 of the password writeback Test Lab Guide](#).

Phase 5: Configure self-service password reset

Follow the instructions in [Phase 3 of the password reset Test Lab Guide](#).

When enabling password reset for the accounts in a specific Azure AD group, add these accounts to the **Password reset** group:

- User 2
- User 3
- User 4
- User 5

Test password reset only for the User 2 account.

Phase 6: Configure multi-factor authentication

Follow the instructions in [Phase 2 of the multi-factor authentication Test Lab Guide](#) for the following user accounts:

- User 2
- User 3

- User 4
- User 5

Test multi-factor authentication only for the User 2 account.

Phase 7: Enable automatic device registration of domain-joined Windows computers

Follow [these instructions](#) to enable automatic device registration of domain-joined Windows computers.

Phase 8: Configure Azure AD password protection

Follow [these instructions](#) to block known weak passwords and their variants.

Phase 9: Enable Azure AD Identity Protection

Follow the instructions in [Phase 2 of the Azure AD Identity Protection Test Lab Guide](#).

Phase 10: Enable modern authentication for Exchange Online and Skype for Business Online

For Exchange Online, follow [these instructions](#).

For Skype for Business Online:

1. Connect to [Skype for Business Online](#).
2. Run this command.

```
Set-CsOauthConfiguration -ClientAdalAuthOverride Allowed
```

3. Verify that the change was successful with this command.

```
Get-CsOauthConfiguration
```

The result is a test environment that meets the requirements of the [Active Directory with password hash sync prerequisite configuration](#) for identity and device access.

Next step

Use [Common identity and device access policies](#) to configure the policies that build on the prerequisites and protect identities and devices.

See also

[Additional identity Test Lab Guides](#)

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Identity and device access prerequisites for pass-through authentication in your Microsoft 365 test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

[Identity and device access configurations](#) are a set of configurations and conditional access policies to protect access to all services in Microsoft 365 for enterprise that are integrated with Azure Active Directory (Azure AD).

This article describes how you can configure a Microsoft 365 test environment that meets the requirements of the [Pass-through authentication prerequisite configuration](#) for identity and device access.

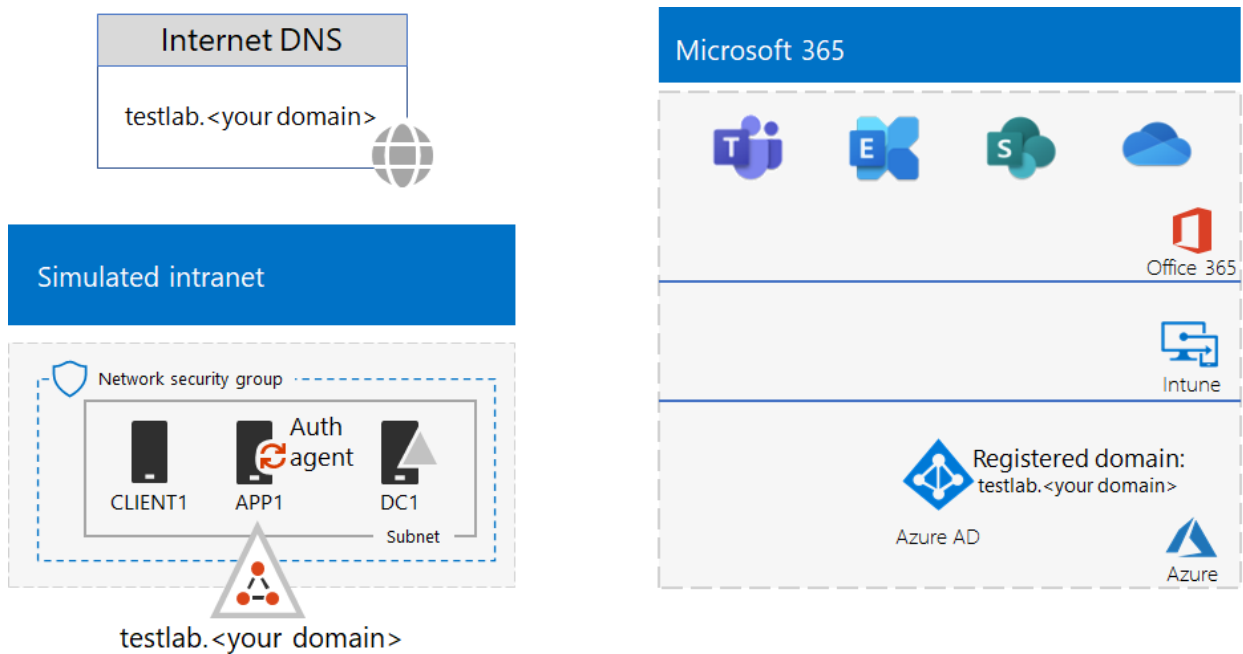
There are ten phases to setting up this test environment:

1. Build out your simulated enterprise with pass-through authentication Microsoft 365 test environment
2. Configure Azure AD seamless single sign-on
3. Configure named locations
4. Configure password writeback
5. Configure self-service password reset
6. Configure multifactor authentication
7. Enable automatic device registration of domain-joined Windows computers
8. Configure Azure AD password protection
9. Enable Azure AD Identity Protection
10. Enable modern authentication for Exchange Online and Skype for Business Online

Phase 1: Build out your simulated enterprise with pass-through authentication Microsoft 365 test environment

Follow the instructions in [Pass-through authentication](#).

Here is the resulting configuration.



Phase 2: Configure Azure AD seamless single sign-on

Follow the instructions in [Phase 2 of the Azure AD Seamless Single Sign-on Test Lab Guide](#).

Phase 3: Configure named locations

First, determine the public IP addresses or address ranges used by your organization.

Next, follow the instructions in [Configure named locations in Azure Active Directory](#) to add the addresses or address ranges as named locations.

Phase 4: Configure password writeback

Follow the instructions in [Phase 2 of the password writeback Test Lab Guide](#).

Phase 5: Configure self-service password reset

Follow the instructions in [Phase 3 of the password reset Test Lab Guide](#).

When enabling password reset for the accounts in a specific Azure AD group, add these accounts to the **Password reset** group:

- User 2
- User 3
- User 4
- User 5

Test password reset only for the User 2 account.

Phase 6: Configure multi-factor authentication

Follow the instructions in [Phase 2 of the multi-factor authentication Test Lab Guide](#) for the following user accounts:

- User 2
- User 3
- User 4

- User 5

Test multi-factor authentication only for the User 2 account.

Phase 7: Enable automatic device registration of domain-joined Windows computers

Follow [these instructions](#) to enable automatic device registration of domain-joined Windows computers.

Phase 8: Configure Azure AD password protection

Follow [these instructions](#) to block known weak passwords and their variants.

Phase 9: Enable Azure AD Identity Protection

Follow the instructions in [Phase 2 of the Azure AD Identity Protection Test Lab Guide](#).

Phase 10: Enable modern authentication for Exchange Online and Skype for Business Online

For Exchange Online, follow [these instructions](#).

For Skype for Business Online:

1. Connect to [Skype for Business Online](#).
2. Run this command.

```
Set-CsOauthConfiguration -ClientAdalAuthOverride Allowed
```

3. Verify that the change was successful with this command.

```
Get-CsOauthConfiguration
```

The result is a test environment that meets the requirements of the [Pass-through authentication prerequisite configuration](#) for identity and device access.

Next step

Use [Common identity and device access policies](#) to configure the policies that build on the prerequisites and protect identities and devices.

See also

[Additional identity Test Lab Guides](#)

[Deploy identity](#)

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Enroll iOS and Android devices in your Microsoft 365 for enterprise test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

This article describes how to enroll and test basic mobile device management capabilities for iOS/iPadOS and Android devices in your Microsoft 365 for enterprise test environment.

Enrolling iOS/iPadOS and Android devices in your test environment involves three phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Enroll your iOS/iPadOS and Android devices](#)
- [Phase 3: Manage your iOS/iPadOS and Android devices remotely](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you want to enroll iOS/iPadOS and Android devices in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to enroll iOS/iPadOS and Android devices in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing automated licensing and group membership doesn't require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It's provided here as an option so that you can test automated licensing and group membership, and you can experiment with it in an environment that represents a typical organization.

Phase 2: Enroll your iOS and Android devices

If you're considering a mobile device management (MDM) solution to manage your devices, you can use Microsoft Intune. When working with any MDM provider, including Intune, devices are "enrolled". When enrolled, they receive the features and settings you configure.

In Intune, there are a few ways to enroll your iOS/iPadOS and Android devices. You can choose the enrollment option that works best for your organization. For more information and guidance, see the following articles:

- [Deployment guide: Enroll iOS and iPadOS devices in Microsoft Intune](#)

- [Deployment guide: Enroll Android devices in Microsoft Intune](#)

If you're ready to use Intune for device management, and want some guidance, then the following information may help:

- [Device management overview](#)
- [Tutorial: Walkthrough Intune in Microsoft Endpoint Manager](#)
- [Deployment guide: Setup or move to Microsoft Intune](#)

Phase 3: Manage your iOS and Android devices remotely

Microsoft Intune provides remote lock and passcode reset feature. If someone loses their device, you can remotely lock the device. If someone forgets their passcode, you can remotely reset it.

- To remotely lock an iOS/iPadOS or Android device, see [Remotely lock devices with Intune](#).
- To remotely reset the passcode, see [Reset or remove a device passcode in Intune](#).

For additional tasks you can run remotely, see [available device actions](#).

Next step

Explore additional [mobile device management](#) features and capabilities in your test environment.

See Also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Device compliance policies for your Microsoft 365 for enterprise test environment](#)

[Microsoft 365 for enterprise overview](#)

Device compliance policies for your Microsoft 365 for enterprise test environment

10/28/2022 • 2 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

This article describes how to add an Intune device compliance policy for Windows 10 devices and Microsoft 365 Apps for enterprise to your Microsoft 365 for enterprise test environment.

Adding an Intune device compliance policy involves two phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Create a device compliance policy for Windows 10 devices](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you want to configure MAM policies in only a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure MAM policies in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing automated licensing and group membership doesn't require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It's provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Create a device compliance policy for Windows 10 devices

In this phase, you create a device compliance policy for Windows 10 devices. This phase uses Microsoft Intune and the [Microsoft Endpoint Manager admin center](#) to add a group, and create a compliance policy.

1. Go to the [Microsoft 365 admin center](#), sign in to your Microsoft 365 test lab subscription with your global administrator account, and select the [Endpoint Manager admin center](#).

If a message similar to **You haven't enabled device management yet** message is shown, then select Intune as the MDM authority. For the specific steps, see [Set the mobile device management authority](#).

The Endpoint Manager admin center focuses on device management and app management. For a tour of

this admin center, see [Tutorial: Walkthrough Intune in Microsoft Endpoint Manager](#).

2. In **Groups**, add a new **Microsoft 365** or **Security** group named **Managed Windows 10 device users**, with an **Assigned** membership type. In the next steps, you'll assign your compliance policy to this group.

For the specific steps, and for information on **Microsoft 365** or **Security** groups, see [Add groups to organize users and devices](#).

3. In **Devices**, create a Windows 10 compliance policy. Assign this policy to the **Managed Windows 10 device users** group you created.

In your policy, you can block simple passwords, require a firewall, require the Microsoft Defender Antimalware service be running, and more. A compliance policy typically includes the base settings, or bare minimum that every device should have.

For the specific steps, and for information on the available compliance settings you can configure, see [Use compliance policies to set rules for devices you manage](#).

When finished, you have a device compliance policy for testing members in the **Managed Windows 10 device users** group.

Next step

Explore additional [mobile device management](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#).

[Enroll iOS and Android devices in your Microsoft 365 for enterprise test environment](#)

[Microsoft 365 for enterprise overview](#)

[Enterprise Mobility + Security \(EMS\)](#)

Increased Microsoft 365 security for your Microsoft 365 for enterprise test environment

10/28/2022 • 4 minutes to read • [Edit Online](#)

This Test Lab Guide can only be used for Microsoft 365 for enterprise test environments.

With the instructions in this article, you configure additional Microsoft 365 settings to increase security in your Microsoft 365 for enterprise test environment.



TIP

Click [here](#) for a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack.

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you just want to configure increased Microsoft 365 security in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure increased Microsoft 365 security in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing increased Microsoft 365 security does not require the simulated enterprise test environment, which includes a simulated intranet connected to the Internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It is provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Configure increased Microsoft 365 security

In this phase, you enable increased Microsoft 365 security for your Microsoft 365 for enterprise test environment. For additional details and settings, see [Configure your tenant for increased security](#).

Configure SharePoint Online to block apps that don't support modern authentication

Apps that do not support modern authentication cannot have [identity and device access configurations](#) applied to them, which is an important element of securing your Microsoft 365 subscription and its digital assets.

1. Go to the [Microsoft 365 admin center](#) and sign in to your Microsoft 365 test lab subscription with your global administrator account.
 - If you are using the lightweight Microsoft 365 test environment, sign in from your local computer.
 - If you are using the simulated enterprise Microsoft 365 test environment, use the [Azure portal](#) to connect to the CLIENT1 virtual machine, and then sign in from CLIENT1.

2. On the new **Microsoft 365 admin center** tab, under **Admin centers** in the left navigation pane, click **SharePoint**.
3. On the new **SharePoint admin center** tab, select **Policies** > **Access control**.
4. Select **Apps that don't support modern authentication**, select **Block access**, and then select **Save**.

Enable Defender for Office 365 for SharePoint, OneDrive for Business, and Microsoft Teams

Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams protects your organization from inadvertently sharing malicious files.

1. Go to the [Security & Compliance Center](#) and sign in with your global administrator account.
2. In the left navigation pane, under **Threat management**, click **Policy**, and then click **Safe Attachments**.
3. Under **Protect files in SharePoint, OneDrive, and Microsoft Teams**, select **Turn on ATP for SharePoint, OneDrive, and Microsoft Teams**.
4. Click **Save**.

Enable anti-malware

Malware is comprised of viruses and spyware. Viruses infect other programs and data, and they spread throughout your computer looking for programs to infect. Spyware refers to malware that gathers your personal information, such as sign-in information and personal data, and sends it back to the malware author.

Microsoft 365 has built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect you from spam. For more information, see [Anti-spam & anti-malware protection](#).

To ensure that anti-malware processing is being performed on files with common attachment file types:

1. Click the back button on your browser to get back to the **Policy** page.
2. Click **Anti-malware**.
3. Double-click the policy named **Default**.
4. In the **Anti-malware policy** window, click **Settings**.
5. Under **Common Attachment Types filter**, select **On**, and then click **Save**.

Phase 3: Examine the security dashboard

Threat management in Microsoft 365 can help you control and manage mobile device access to your organization's data, help protect your organization from data loss, and help protect inbound and outbound messages from malicious software and spam. You also use threat management to protect your domain's reputation and to determine whether or not senders are maliciously spoofing accounts from your domain.

To see the security dashboard:

1. If needed, go to the [Security & Compliance Center](#) and sign in with your global administrator account.
2. In the left navigation pane, under **Threat management**, click **Dashboard**.

Take a close look at all the cards on the dashboard to familiarize yourself with the information provided.

For more information, see [Security Dashboard](#).

Phase 4: Examine Microsoft Secure Score

Microsoft Secure Score shows your security posture as a number, which indicates your current level relative to the features that are available in your subscription. It also gives you a list of improvement actions you can take to improve your score.

1. Create a new tab in your browser, go to the [Microsoft 365 Defender portal](#), and then click **Secure score**.
2. On the **Overview** tab, note your current Secure Score and how it compares with the global average and subscriptions with a similar number of licenses.
3. On the **Improvement actions** tab, read through the list of actions you can take to increase your score.

For more information, see [Microsoft Secure Score](#).

Next steps

Explore additional [information protection](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Data classification for your Microsoft 365 for enterprise test environment

10/28/2022 • 3 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

This article describes how to configure data classification using retention labels in your Microsoft 365 for enterprise test environment.

Classifying data in your test environment involves three phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Create retention labels](#)
- [Phase 3: Apply retention labels to documents](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you just want to configure retention labels in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure retention labels in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing retention labels doesn't require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services (AD DS) forest. It's provided here as an option so that you can test automated licensing and group membership and experiment with it in an environment that represents a typical organization.

Phase 2: Create retention labels

In this phase, create the retention labels for the different levels of retention for SharePoint Online documents folders:

1. Sign in to the [Microsoft 365 Defender portal](#) with your global admin account.
2. From the Home - Microsoft 365 security tab of your browser, select **Classification** > **Retention labels**.
3. Select **Create a label**.

4. In the **Name your label** pane, enter **Internal Public** in **Name your label**, and then select **Next**.
5. In the **File plan descriptors** pane, select **Next**.
6. In the **Label settings** pane, if needed, set **Retention** to **On**, and then select **Next**.
7. In the **Review your settings** pane, select **Create the label**.
8. Repeat steps 3-7 for additional labels with these names:

- Private
- Sensitive
- Highly Confidential

1. In the **Retention labels** pane, select **Publish labels**.
2. In the **Choose labels to publish** pane, select **Choose labels to publish**.
3. In the **Choose labels** pane, select **Add** and select all four labels.
4. Select **Add**, and then select **Done**.
5. On the **Choose labels to publish** pane, select **Next**.
6. On the **Choose locations** pane, select **Next**.
7. On the **Name your policy** pane, enter **Example organization** in **Name**, and then select **Next**.
8. On the **Review your settings** pane, select **Publish labels**.

It might take a few minutes for the retention labels to be published.

Phase 3: Apply retention labels to documents

In this phase, you discover the default retention label behavior for files in the Documents folder of a SharePoint Online site and manually change the retention label of a document.

First, create a sensitive-level SharePoint Online team site:

1. Using a private instance of your browser, sign in to the [Microsoft 365 admin center](#) using your global admin account.
2. In the list of tiles, select **SharePoint**.
3. On the new **SharePoint** tab in your browser, select **Create site**.
4. On the **Create a site** page, select **Team site**.
5. In the **Team site name** box, enter **SensitiveFiles**.
6. In the **Team site description** box, enter **SharePoint site for sensitive files**.
7. In **Privacy settings**, select **Private - only members can access this site**, and then select **Next**.
8. In the **Who do you want to add?** pane, select **Finish**.

Next, configure the Documents folder of the SensitiveFiles team site for the Sensitive retention label.

1. In the **SensitiveFiles** tab of your browser, select **Documents**.
2. Select the **Settings** icon, and then select **Library settings**.
3. Under **Permissions and Management**, select **Apply label to items in this list or library**. If this option doesn't appear, your retention labels aren't yet published. Try this step at a later time.
4. In **Settings-Apply Label**, select **Sensitive** in the drop-down box, and then select **Save**.

Next, create a new document in the SensitiveFiles site and change its retention label.

1. In the documents folder, select **New > Word document**.
2. Enter some text in the blank document. Wait for the text to be saved.
3. On the menu bar, select **Shared Documents**.
4. Next to the **Document.docx** file name, select the vertical ellipsis, and then select **Details**.

5. In the right pane, in the **Properties** section, under **Apply retention label**, note that the document has had the **Sensitive** retention label automatically applied.
6. Click **Edit all**.
7. In the **Document.docx** pane, under **Apply retention label**, select the **Highly Confidential** label, and then select **Save**.

Next step

Explore additional [information protection](#) features and capabilities in your test environment.

See also

[Microsoft 365 for enterprise Test Lab Guides](#)

[Microsoft 365 for enterprise overview](#)

[Microsoft 365 for enterprise documentation](#)

Privileged access management for your Microsoft 365 for enterprise test environment

10/28/2022 • 5 minutes to read • [Edit Online](#)

This Test Lab Guide can be used for both Microsoft 365 for enterprise and Office 365 Enterprise test environments.

This article describes how to configure privileged access management to increase security in your Microsoft 365 for enterprise test environment.

Configuring privileged access management involves three phases:

- [Phase 1: Build out your Microsoft 365 for enterprise test environment](#)
- [Phase 2: Configure privileged access management](#)
- [Phase 3: Verify that approval is required for elevated and privileged tasks](#)



TIP

For a visual map to all the articles in the Microsoft 365 for enterprise Test Lab Guide stack, go to [Microsoft 365 for enterprise Test Lab Guide Stack](#).

Phase 1: Build out your Microsoft 365 for enterprise test environment

If you want to configure privileged access management in a lightweight way with the minimum requirements, follow the instructions in [Lightweight base configuration](#).

If you want to configure privileged access management in a simulated enterprise, follow the instructions in [Pass-through authentication](#).

NOTE

Testing privileged access management doesn't require the simulated enterprise test environment, which includes a simulated intranet connected to the internet and directory synchronization for an Active Directory Domain Services forest. It's provided here as an option so that you can test privileged access management and experiment with it in an environment that represents a typical organization.

Phase 2: Configure privileged access management

In this phase, configure an approvers group and enable privileged access management for your Microsoft 365 for enterprise test environment. For additional details and an overview of privileged access management, see [Privileged access management](#).

To set up and use privileged access in your organization, perform the following steps.

Step 1: Create an approver's group

Before you start using privileged access, determine who will have approval authority for incoming requests for access to elevated and privileged tasks. All users who are part of the Approvers' group can approve access requests. To use privileged access, you must create a mail-enabled security group in Microsoft 365. In your test environment, name the new security group "Privileged Access Approvers" and add the "User 3" that was previously created in previous test lab guide steps.

Step 2: Enable privileged access

Privileged access needs to be explicitly turned on in Microsoft 365 with the default approver group, and it must include a set of system accounts that you want excluded from the privileged access management access control. Be sure to enable privileged access in your organization before starting Phase 3 of this guide.

Phase 3: Verify that approval is required for elevated and privileged tasks

In this phase, verify that the privileged access policy is working and that users require approval to execute defined elevated and privileged tasks.

Test the ability to execute a task NOT defined in a privileged access policy

First, attempt to create a new Journal rule in Exchange Online PowerShell. The [New-JournalRule](#) task is not currently defined in a privileged access policy for your organization.

1. On your local computer, [Connect to Exchange Online PowerShell](#) using credentials with the Exchange Role Management role for your test environment.
2. Create a new Journal rule for your organization by running the following command:

```
New-JournalRule -Name "JournalRule1" -Recipient joe@contoso.onmicrosoft.com -JournalEmailAddress barbara@adatum.com -Scope Global -Enabled $true
```

3. Verify that the new Journal Rule was successfully created:

```
Get-JournalRule -Identity "JournalRule1"
```

Create a new privileged access policy for the New-JournalRule task

NOTE

If you haven't already completed the Steps 1 and 2 from Phase 2 of this guide, be sure follow the steps to create an approver's group named "Privilege Access Approvers" to enable privileged access in your test environment.

1. Sign in to the [Microsoft 365 admin center](#) using credentials with the Exchange Role Management role for your test environment.
2. In the Admin Center, go to **Settings > Security & Privacy > Privileged access**.
3. Select **Manage access policies and requests**.
4. Select **Configure policies**, and then select **Add a policy**.
5. From the drop-down fields, select or enter the following values:

Policy type: Task **Policy scope:** Exchange **Policy name:** New Journal Rule **Approval type:** Manual
Approval group: Privileged Access Approvers

6. Select **Create**, and then select **Close**. It may take a few minutes for the policy to be fully configured and

enabled. Be sure to allow time for the policy to be fully enabled before testing the approval requirement in the next step.

Test approval requirement for the New-JournalRule task defined in a privileged access policy

1. On your local computer, [Connect to Exchange Online PowerShell](#) using credentials with the Exchange Role Management role for your test environment.
2. In Exchange Online PowerShell, create a new Journal rule for your organization:

```
New-JournalRule -Name "JournalRule2" -Recipient user1@<your subscription domain> -JournalEmailAddress user1@<your subscription domain> -Scope Global -Enabled $true
```

3. View the "Insufficient permissions" error in Exchange Online PowerShell:

```
Insufficient permissions. Please raise an elevated access request for this task.
+ CategoryInfo          : NotSpecified: (:) [], LocalizedException
+ FullyQualifiedErrorId : [Server=CY1PR00MB0220,RequestId=7b8c7470-ddd0-4528-a01e-5e20ecc9bd54,TimeStamp=9/19/2018 7:38:34 PM] [FailureCategory=Cmdlet-LocalizedException] 882BD051
+ PSComputerName        : outlook.office365.com
```

Request access to create a new Journal Rule using the New-JournalRule task

1. Sign in to the [Microsoft 365 admin center](#) using credentials with the Exchange Role Management role for your test environment.
2. In the Admin Center, go to **Settings > Security & Privacy > Privileged access**.
3. Select **Manage access policies and requests**.
4. Select **New request**. From the drop-down fields, select the appropriate values for your organization:

Request type: Task **Request scope:** Exchange **Request for:** New Journal Rule **Duration (hours):** 2
Comments: Request permission to create a new Journal Rule

5. Select **Save**, and then select **Close**. Your request will be sent to the approver's group via email.

Approve privileged access request for the creation of a new Journal Rule

1. Sign in to the [Microsoft 365 admin center](#) using the credentials for User 3 in your test environment (member of the "Privileged Access Approvers" security group in your test environment).
2. In the Admin Center, go to **Settings > Security & Privacy > Privileged access**.
3. Select **Manage access policies and requests**.
4. Select the pending request, and then select **Approve** to grant access to the user account to create a new Journal Rule. The account (the requesting user) will receive an email confirmation that approval was granted.

Test creating a new Journal Rule with privileged access approved for the New-JournalRule task

1. On your local computer, [Connect to Exchange Online PowerShell](#) using credentials with the Exchange Role Management role for your test environment.
2. In Exchange Online PowerShell, create a new Journal rule for your organization:

```
New-JournalRule -Name "JournalRule2" -Recipient user1@<your subscription domain> -JournalEmailAddress user1@<your subscription domain> -Scope Global -Enabled $true
```

3. Verify that the new Journal rule was successfully created:

```
Get-JournalRule -Identity "JournalRule2"
```

Next step

Explore additional [information protection](#) features and capabilities in your test environment.

See also

- [Microsoft 365 for enterprise Test Lab Guides](#)
- [Microsoft 365 for enterprise overview](#)
- [Microsoft 365 for enterprise documentation](#)

Microsoft 365 for enterprise for the Contoso Corporation

10/28/2022 • 2 minutes to read • [Edit Online](#)

Microsoft 365 for enterprise is the Microsoft premier cloud offering that combines local and cloud-based productivity apps and services with Windows 10 Enterprise and advanced security features. It's a complete, intelligent solution that enables everyone to work together creatively and securely.

Contoso Corporation is a fictional but representative global manufacturing conglomerate with its headquarters in Paris. The company deployed Microsoft 365 for enterprise and addressed major design decisions and implementation details for networking, identity, Windows 10 Enterprise, Microsoft 365 Apps for enterprise, mobile device management, information protection, and security.

The company's overall goal for Microsoft 365 for enterprise is to accelerate its digital transformation by using cloud services to bring together its employees, partners, data, and processes to create customer value and maintain its competitive advantage in a digital-first world.

See these articles for the details:

- [Overview](#)

Contoso is a global manufacturing, sales, and support organization with more than 100,000 products.

- [Contoso IT infrastructure and needs](#)

Contoso is transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive setup that incorporates cloud-based personal productivity workloads, applications, and hybrid scenarios.

- [Networking](#)

Contoso network engineers optimized traffic for their on-premises users to their intranet edge and to the closest Microsoft network location on the internet.

- [Identity](#)

The Contoso identity-in-the-cloud solution leverages the company's on-premises Active Directory Domain Services (AD DS) forest. It includes federated authentication with their existing trusted, third-party identity providers.

- [Windows 10 Enterprise](#)

The Contoso infrastructure for Windows 10 Enterprise deploys and automatically installs updates for devices that are running the company's primary PC and device operating system.

- [Microsoft 365 Apps for enterprise](#)

The Contoso infrastructure for Microsoft 365 Apps for enterprise deploys and automatically installs updates for the Microsoft Office suite of productivity software.

- [Mobile device management](#)

With many roaming employees who have both company and personal smart phones and tablets, Contoso uses mobile device management to enroll and secure devices and their data and manage apps.

- [Information protection](#)

To ensure that both common and high-value data are identified, labeled, and subject to layers of security, Contoso enforces its data-security policies with Microsoft 365 for enterprise information protection.

- [Summary of Microsoft 365 for enterprise security](#)

Contoso uses the full spectrum of Microsoft 365 for enterprise security features for identity and access management, threat protection, information protection, and security management.

See these additional IT scenarios and configurations:

- [COVID-19 response and infrastructure for remote and onsite work](#)

Learn how Contoso updated their remote access capability and their new installs and updates infrastructure for remote and onsite workers.

- [Team for a top-secret project](#)

To create a secure collaboration environment for a top-secret project, Contoso used a team with security isolation.

- [Teams voice migration](#)

Learn how Contoso migrated their on-premises users to Microsoft Teams for unified communication, collaboration, and voice.

- [Communication compliance offensive language policy](#)

Learn how Contoso quickly configured an offensive language policy for Microsoft Teams, Exchange, and Yammer communications.

Next step

Learn [about the Contoso Corporation](#) and the design considerations that were addressed when they deployed Microsoft 365 for enterprise.

See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Overview of Contoso Corporation

10/28/2022 • 2 minutes to read • [Edit Online](#)

The Contoso Corporation is a multinational business with its headquarters in Paris. The company is a manufacturing, sales, and support organization with more than 100,000 products.

Contoso around the world

Figure 1 shows the headquarters office in Paris and regional hub and satellite offices on various continents.

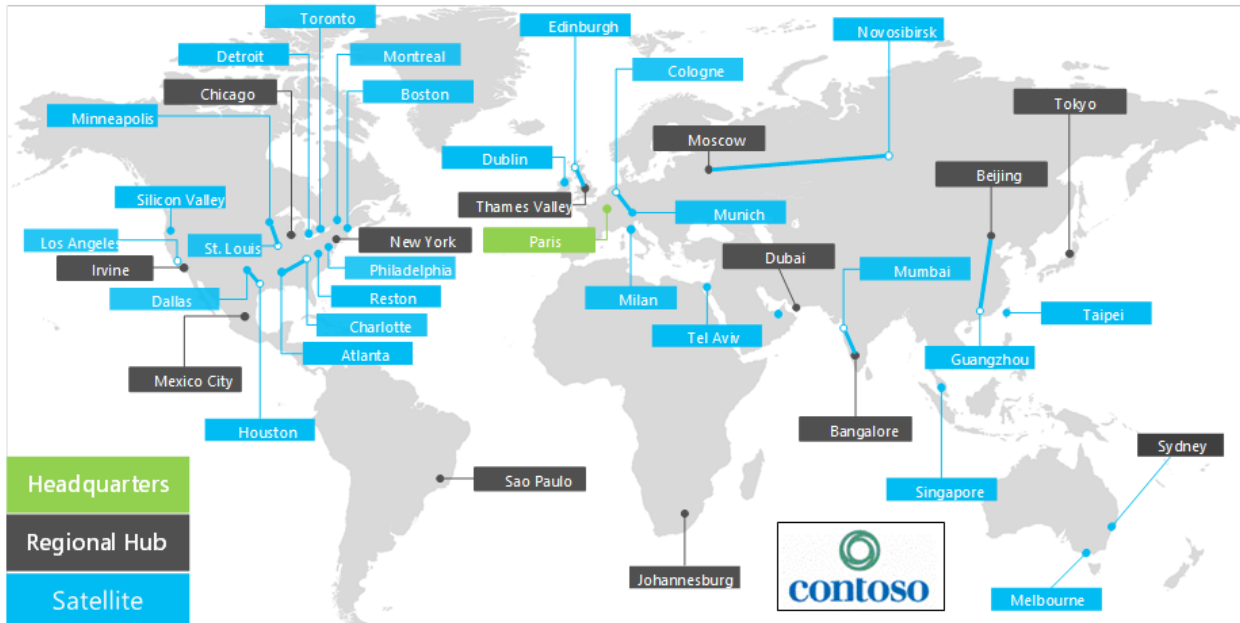


Figure 1: Contoso offices around the world

Contoso has three tiers of offices:

- Headquarters

Contoso headquarters is a corporate campus on the outskirts of Paris with dozens of buildings for administrative, engineering, and manufacturing facilities. All the Contoso datacenters and its internet presence are housed in the Paris headquarters.

The headquarters has 25,000 workers.

- Regional hubs

Hub offices serve a specific region of the world with 60-percent sales and support staff. Each regional hub is connected to the Paris headquarters through a high-bandwidth WAN link.

The regional hubs have an average of 2,000 workers.

- Satellite offices

Satellite offices contain 80-percent sales and support staff. They provide an on-site presence for Contoso customers in key cities or subregions. Each satellite office is connected to a regional hub through a high-bandwidth WAN link.

The satellite offices have an average of 250 workers.

About 25 percent of the Contoso workforce is mobile-only. The regional hubs and satellite offices have a higher percentage of these workers. Providing better support for mobile-only workers is an important business goal for Contoso.

Design considerations for Microsoft 365 for enterprise

The Contoso IT architects identified the following design-requirement factors for deploying Microsoft 365 for enterprise:

- Multiple geographic locations with local regulations and compliance requirements
- A central intranet datacenter in the headquarters office and regional application servers that host internal line-of-business applications
- An existing Microsoft Endpoint Configuration Manager infrastructure
- A mix of client computing devices that run Windows, Mac, and Linux
- A mix of personal and company-owned mobile devices, including iOS (iPhone and iPad) and Android smart phones and tablets
- Many remote and mobile workers
- Many business partners
- A large amount of customer and other confidential personal information to manage and secure
- A large amount of high-value intellectual property in the form of design specifications for products and manufacturing trade secrets

Next step

Learn about the Contoso Corporation [on-premises IT infrastructure](#) and how the company's business needs are addressed with Microsoft 365 for enterprise.

See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Contoso IT infrastructure and business needs

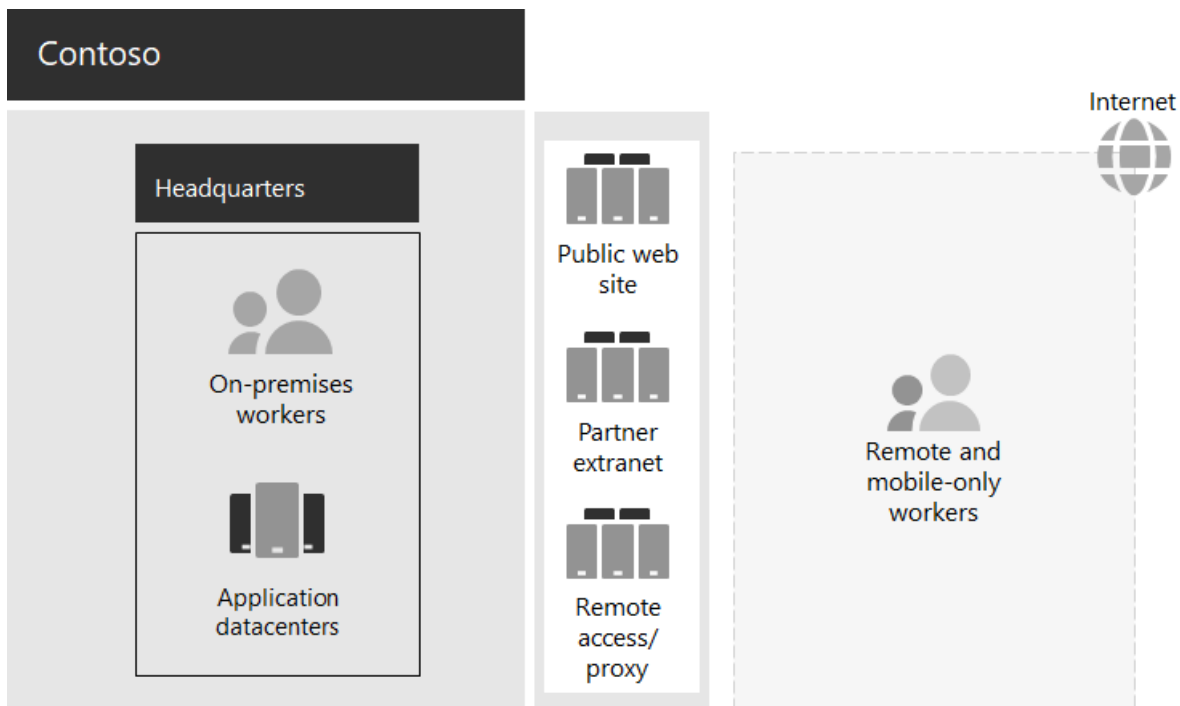
10/28/2022 • 3 minutes to read • [Edit Online](#)

Contoso is transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive setup that incorporates cloud-based personal productivity workloads and applications.

Existing Contoso IT infrastructure

Contoso uses a mostly centralized on-premises IT infrastructure, with application datacenters in the Paris headquarters.

Here is the headquarters office with application datacenters, a DMZ, and the internet.



The on-premises application datacenters host:

- Custom line-of-business applications that use SQL Server and other Linux databases.
- A set of legacy SharePoint servers.
- Organization and team-level servers for file storage.

Additionally, each regional hub office supports a set of servers with a similar set of applications. These servers are under the control of regional IT departments.

Searchability across the applications and data of these separate multi-geographical datacenters continues to be a challenge.

In the Contoso headquarters DMZ, different sets of servers provide:

- Hosting for the Contoso public web site, from which customers can order products, parts, supplies, and service.
- Hosting for the Contoso partner extranet for partner communication and collaboration.
- Virtual private network (VPN)-based remote access to the Contoso intranet and web proxying for workers in the Paris headquarters.

Contoso business needs

Contoso business needs fall into five main categories:

Productivity

- Make collaboration easier

Replace email and file share-based collaboration with an online model that allows real-time changes on documents, easier online meetings, and captured conversation threads.

- Improve productivity for remote and mobile workers

With many employees working from home or in the field, replace the bottlenecked VPN solution with performant access to Contoso data and resources in the cloud.

- Increase creativity and innovation

Take advantage of the latest visual learning and idea development methods, including inking and 3D visualization.

Security

- Identity and access management

Enforce multifactor and other forms of authentication and protect user and administrator account credentials.

- Threat protection

Protect against external security threats, including email and operating system-based malware.

- Information protection

Lock down access to and encrypt high-value digital assets, such as customer data, design and manufacturing specifications, and employee information.

- Security management

Monitor security posture and detect and respond to threats in real time.

Remote and mobile access and business partners

- Improve security for remote and mobile workers

Implement bring your own device (BYOD) and company-owned device management to ensure secured access, correct application behavior, and company data protection.

- Reduce remote access infrastructure for employees

Reduce maintenance and support costs and improve performance for remote access solution by moving commonly accessed resources to the cloud.

- Provide better connectivity and lower overhead for business-to-business (B2B) transactions

Replace an aging and expensive partner extranet with a cloud-based solution that uses federated authentication.

Compliance

- Adhere to regional regulatory requirements

Ensure compliance with industry and regional regulations for data storage, encryption, data privacy, and

personal data regulations, such as the General Data Protection Regulation (GDPR) for the Europe Union.

Management

- Lower IT overhead for managing software running on client PCs and devices

Automate installation of updates to the Windows operating system and Microsoft 365 Apps for enterprise across the organization.

Mapping Contoso business needs to Microsoft 365 for enterprise

The Contoso IT department determined the following mapping of business needs to Microsoft 365 E5 features prior to deployment:

CATEGORY	BUSINESS NEED	MICROSOFT 365 FOR ENTERPRISE PRODUCTS OR FEATURES
Productivity		
	Make collaboration easier	Microsoft Teams, SharePoint, OneDrive
	Improve productivity for remote and mobile workers	Microsoft 365 workloads and cloud-based data
	Increase creativity and innovation	Windows Ink, Cortana at Work, PowerPoint
Security		
	Identity & access management	Dedicated global administrator accounts with Azure AD Multi-Factor Authentication (MFA) and Azure AD Privileged Identity Management (PIM) MFA for all user accounts Conditional Access Security Reader Windows Hello Windows Credential Guard
	Threat protection	Advanced Threat Analytics Windows Defender Defender for Office 365 Microsoft Defender for Office 365 Microsoft 365 threat investigation and response
	Information protection	Azure Information Protection Data Loss Prevention (DLP) Windows Information Protection (WIP) Microsoft Defender for Cloud Apps Microsoft Intune
	Security management	Microsoft Defender for Cloud Windows Defender Security Center
Remote and mobile access and business partners		

CATEGORY	BUSINESS NEED	MICROSOFT 365 FOR ENTERPRISE PRODUCTS OR FEATURES
	Better security for remote and mobile workers	Microsoft Intune
	Reduce remote access infrastructure for employees	Microsoft 365 workloads and cloud-based data
	Improve connectivity and lower overhead for B2B transactions	Federated authentication and cloud-based resources
Compliance		
	Adhere to regional regulatory requirements	GDPR features in Microsoft 365
Management		
	Lower IT overhead for installing client updates	Windows 10 Enterprise updates Microsoft 365 Apps for enterprise updates

Next step

Learn about the Contoso Corporation [on-premises network](#) and how it was optimized for access and latency to Microsoft 365 cloud-based resources.

See also

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Networking for the Contoso Corporation

10/28/2022 • 4 minutes to read • [Edit Online](#)

To adopt a cloud-inclusive infrastructure, Contoso devised a fundamental shift in how network traffic to cloud services travels. Instead of an internal hub-and-spoke model that focuses network connectivity and traffic for the next level of the office hierarchy, they mapped user locations to local internet egress and local connections to the closest Microsoft 365 network location on the internet.

Networking infrastructure

These are the network elements that link Contoso offices across the globe:

- Multiprotocol Label Switching (MPLS) WAN network

An MPLS WAN network connects the Paris headquarters to regional offices and regional offices to satellite offices in a spoke-and-hub configuration. The network enables users to access on-premises servers that make up line-of-business applications in the Paris headquarters. It also routes any generic internet traffic to the Paris office, where network security devices scrub the requests. Within each office, routers deliver traffic to wired hosts or wireless access points on subnets, which use the private IP address space.

- Local direct internet access for Microsoft 365 traffic

Each office has a software-defined WAN (SD-WAN) device that has one or more local internet ISP network circuits with its own internet connectivity through a proxy server. This is typically implemented as a WAN link to a local ISP that also provides public IP addresses and a local DNS server.

- Internet presence

Contoso owns the contoso.com public domain name. The Contoso public web site for ordering products is a set of servers in an internet-connected datacenter in the Paris campus. Contoso uses a /24 public IP address range on the internet.

Figure 1 shows the Contoso networking infrastructure and its connections to the internet.

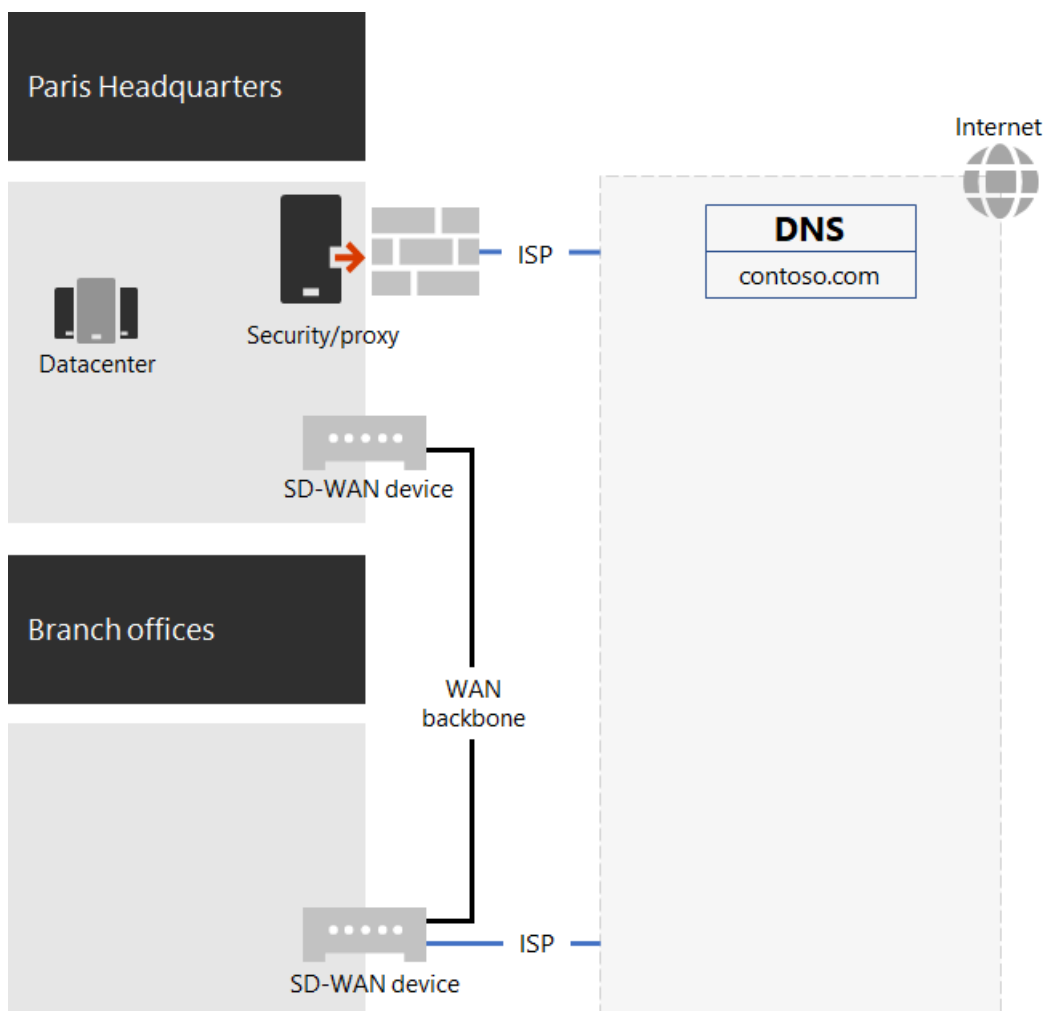


Figure 1: The Contoso network

Use of SD-WAN for optimal network connectivity to Microsoft

Contoso followed [Microsoft 365 network connectivity principles](#) to:

- Identify and differentiate Microsoft 365 network traffic
- Egress network connections locally
- Avoid network hairpins
- Bypass duplicate network security devices

There are three categories of network traffic for Microsoft 365: *Optimize*, *Allow*, and *Default*. Optimize and Allow traffic is trusted network traffic that's encrypted and secured at the endpoints and is destined for the Microsoft 365 network.

Contoso decided to:

- Use direct internet egress for Optimize and Allow category traffic and to forward all Default category traffic to the Paris-based central internet connection.
- Deploy SD-WAN devices at each office as a simple way to follow these principles and achieve optimal network performance for Microsoft 365 cloud-based services.

The SD-WAN devices have a LAN port for the local office network and multiple WAN ports. One WAN port connects to their MPLS network. Another connects to a local ISP circuit. The SD-WAN device routes Optimize and Allow category network traffic over the ISP link.

The Contoso line-of-business app infrastructure

Contoso architected its line-of-business application and server intranet infrastructure for the following:

- Satellite offices use local caching servers to store frequently accessed documents and internal web sites.
- Regional hubs use regional application servers for the regional and satellite offices. These servers synchronize with servers in the Paris headquarters.
- The Paris campus datacenters contain centralized application servers that serve the entire organization.

Figure 2 shows the percentage of network traffic capacity used when accessing servers across the Contoso intranet.

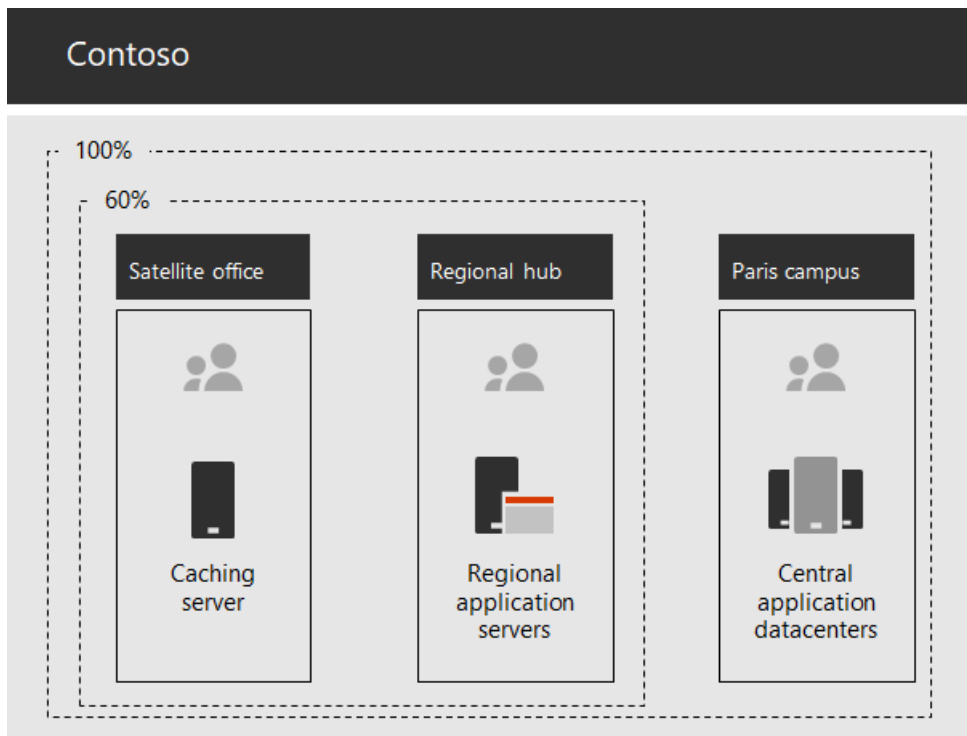


Figure 2: The Contoso infrastructure for internal applications

For the satellite or regional hub offices, 60 percent of the resources needed by employees can be served by satellite and regional hub office servers. The additional 40 percent of resource requests must go over the WAN link to the Paris campus.

Network analysis and preparation for Microsoft 365 for enterprise

Successful adoption of Microsoft 365 for enterprise services by Contoso users depends on highly available and performant connectivity to the internet or directly to Microsoft cloud services. Contoso took these steps to plan and implement optimized connectivity to Microsoft 365 for enterprise cloud services:

1. Create a company WAN network diagram to aid with planning

To start their network planning, Contoso created a diagram showing their office locations, existing network connectivity, existing network perimeter devices, and classes of service that are managed on the network. They used this diagram for each subsequent step in the planning and implementation of networking connectivity.

2. Create a plan for Microsoft 365 for enterprise network connectivity

Contoso used the [Microsoft 365 network connectivity principles](#) and sample reference network architectures to identify SD-WAN as their preferred topology for Microsoft 365 connectivity.

3. Analyze internet-connection utilization and MPLS-WAN bandwidth at each office, and increase bandwidth as needed

Each office's current usage was analyzed, and circuits were increased so that predicted Microsoft 365 cloud-based traffic would operate with an average of 20-percent unused capacity.

4. Optimize performance to Microsoft network services

Contoso determined the set of Office 365, Intune, and Azure endpoints and configured firewalls, security devices, and other systems in the internet path for optimal performance. Endpoints for Office 365 Optimize and Allow category traffic were configured into the SD-WAN devices for routing over the ISP circuit.

5. Configure internal DNS

DNS is required to be functional and to be looked up locally for Microsoft 365 traffic.

6. Validate network endpoint and port connectivity

Contoso ran Microsoft network connectivity test tools to validate connectivity for Microsoft 365 for enterprise cloud services.

7. Optimize employee computers for network connectivity

Individual computers were checked to ensure that the latest operating system updates were installed and that endpoint security monitoring was active on all clients.

Next step

Learn how Contoso is [leveraging its on-premises Active Directory Domain Services in the cloud](#) for employees and federating authentication for customers and business partners.

See also

[Networking roadmap for Microsoft 365](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Identity for the Contoso Corporation

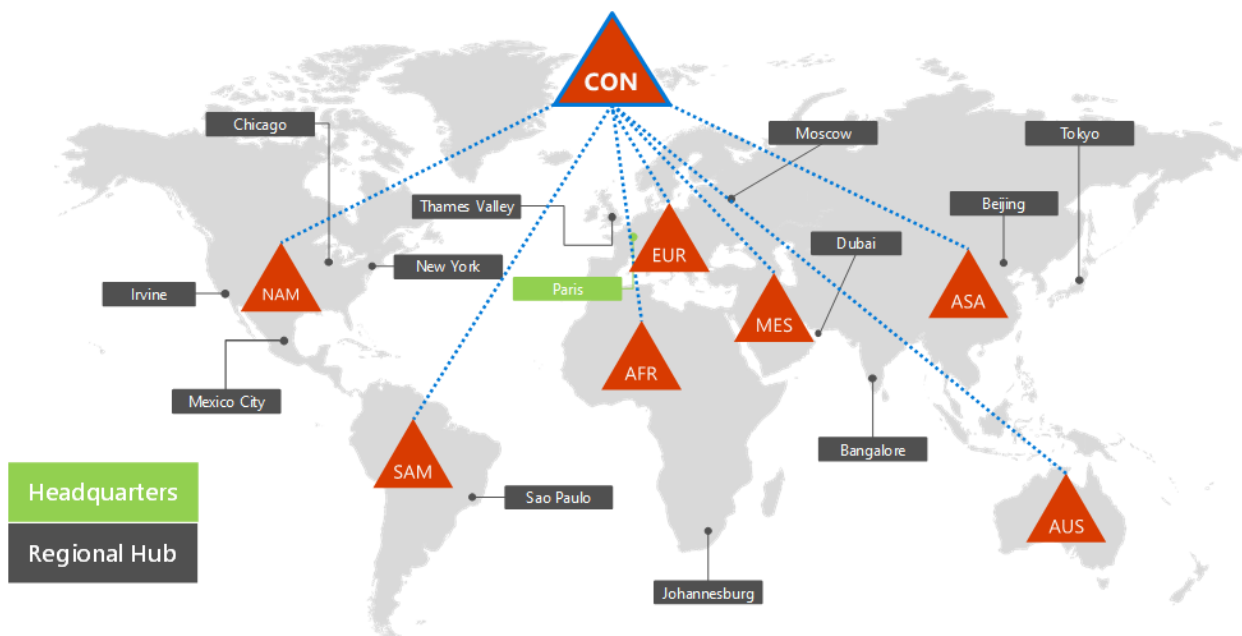
10/28/2022 • 2 minutes to read • [Edit Online](#)

Microsoft provides Identity as a Service (IDaaS) across its cloud offerings through Azure Active Directory (Azure AD). To adopt Microsoft 365 for enterprise, the Contoso IDaaS solution had to use their on-premises identity provider and include federated authentication with their existing trusted, third-party identity providers.

The Contoso Active Directory Domain Services forest

Contoso uses a single Active Directory Domain Services (AD DS) forest for contoso.com with seven subdomains, one for each region of the world. The headquarters, regional hub offices, and satellite offices contain domain controllers for local authentication and authorization.

Here's the Contoso forest with regional domains for the different parts of the world that contain regional hubs.



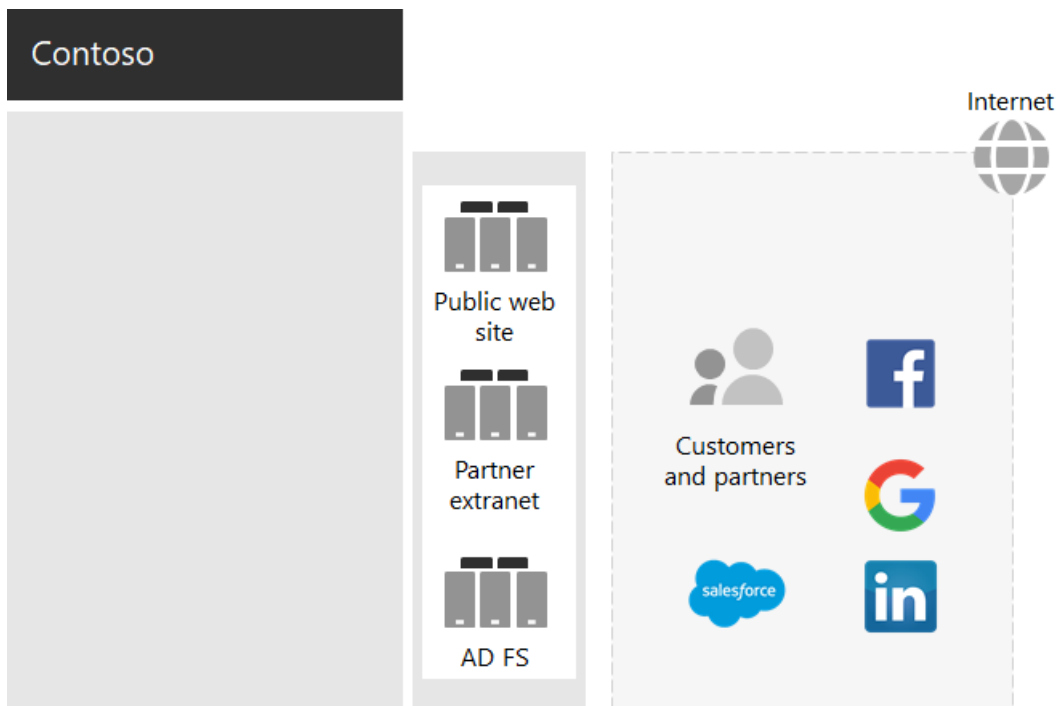
Contoso decided to use the accounts and groups in the contoso.com forest for authentication and authorization for its Microsoft 365 workloads and services.

The Contoso federated authentication infrastructure

Contoso allows:

- Customers to use their Microsoft, Facebook, or Google Mail accounts to sign in to the company's public web site.
- Vendors and partners to use their LinkedIn, Salesforce, or Google Mail accounts to sign in to the company's partner extranet.

Here's the Contoso DMZ containing a public web site, a partner extranet, and a set of Active Directory Federation Services (AD FS) servers. The DMZ is connected to the internet that contains customers, partners, and internet services.



AD FS servers in the DMZ facilitate authentication of customer credentials by their identity providers for access to the public web site and partner credentials for access to the partner extranet.

Contoso decided to keep this infrastructure and dedicate it to customer and partner authentication. Contoso identity architects are investigating the conversion of this infrastructure to Azure AD [B2B](#) and [B2C](#) solutions.

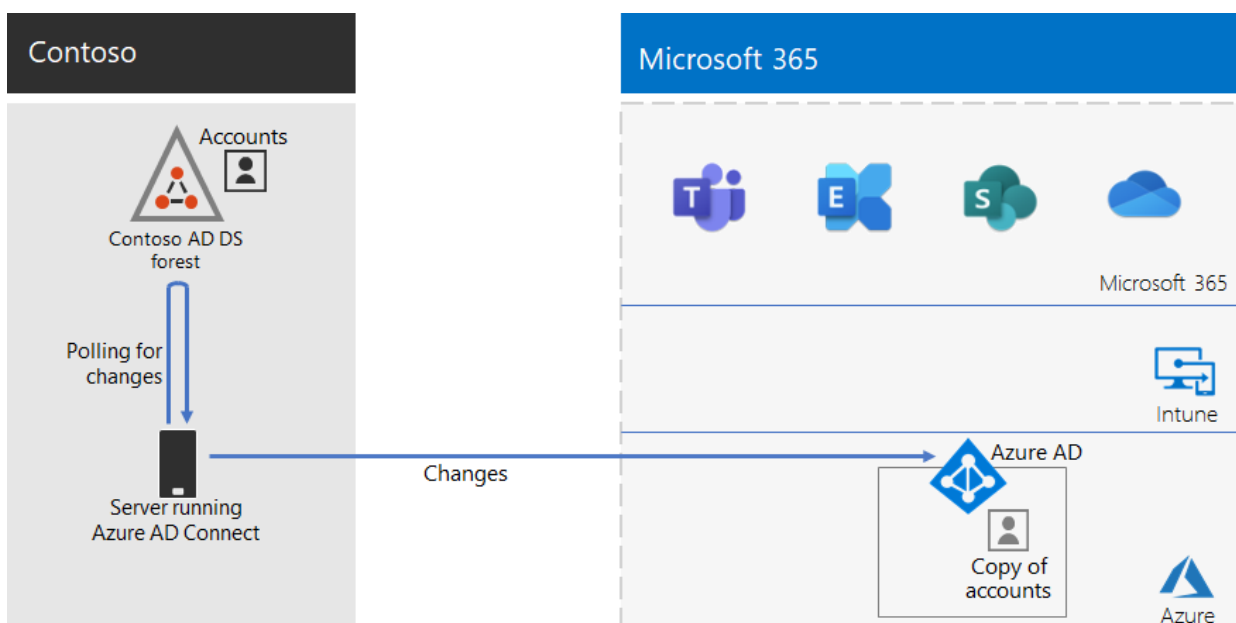
Hybrid identity with password hash synchronization for cloud-based authentication

Contoso wanted to use its on-premises AD DS forest for authentication to Microsoft 365 cloud resources. It decided to use password hash synchronization (PHS).

PHS synchronizes the on-premises AD DS forest with the Azure AD tenant of their Microsoft 365 for enterprise subscription, copying user and group accounts and a hashed version of user account passwords.

To do directory synchronization, Contoso deployed the Azure AD Connect tool on a server in its Paris datacenter.

Here's the server running Azure AD Connect polling the Contoso AD DS forest for changes and then synchronizing those changes with the Azure AD tenant.

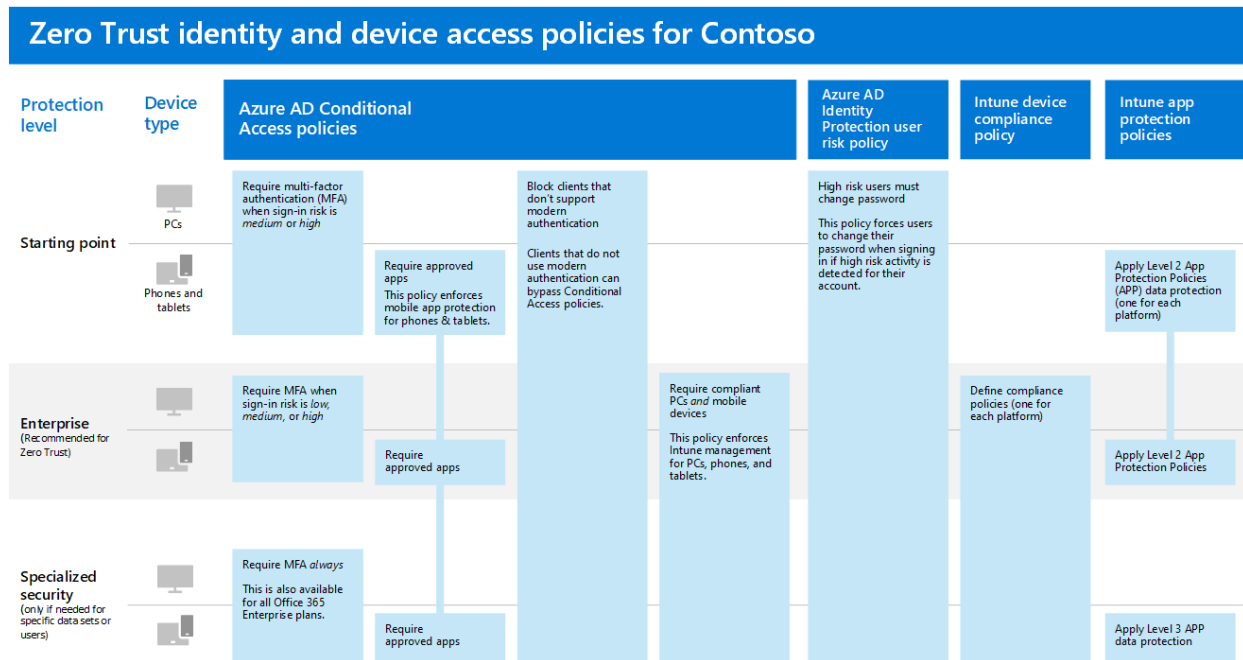


Conditional Access policies for Zero Trust identity and device access

Contoso created a set of Azure AD and Intune [Conditional Access policies](#) for three protection levels:

- *Starting point* protections apply to all user accounts.
- *Enterprise* protections apply to senior leadership and executive staff.
- *Specialized security* protections apply to specific users in the finance, legal, and research departments who have access to highly regulated data.

Here's the resulting set of Contoso identity and device Conditional Access policies.



Next step

Learn how Contoso uses its Microsoft Endpoint Configuration Manager infrastructure to [deploy and keep current Windows 10 Enterprise](#) across its organization.

See also

[Deploy identity for Microsoft 365](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Windows 10 Enterprise deployment for Contoso

10/28/2022 • 3 minutes to read • [Edit Online](#)

Prior to the wide rollout of Microsoft 365 for enterprise, Contoso had Windows-compatible PCs and devices running a mixture of Windows 7 (10%), Windows 8.1 (65%), and Windows 10 (25%). Contoso wanted to upgrade their PCs for Windows 10 Enterprise take advantage of advanced security and lowered IT overhead from automated deployments of updates.

After assessing their infrastructure and business needs, Contoso identified these key requirements for the deployment:

- As many PCs and devices as possible should run Windows 10 Enterprise
- Rollout of the in-place upgrades leverages existing Configuration Manager infrastructure
- Control over which versions of Windows 10 Enterprise to deploy and updates are done through rings
- PCs and devices should stay up to date with minimal IT administrative costs and with minimal impact to end-users

Up to date is defined as the supported version of Windows 10 Enterprise that meets Contoso's business needs, which can be different from having all Windows-compatible PCs running the latest version of Windows 10 Enterprise.

Deployment tools

Prior to and during in-place upgrades of Windows 10 Enterprise, Contoso used the following solutions of Windows Analytics:

- Upgrade Readiness

Collects system, application, and driver data for analysis, and then identifies compatibility issues that can block an upgrade and suggested fixes the issues are known to Microsoft.

- Update Compliance

Shows you the state of your devices with respect to the Windows updates so that you can ensure that they are on the most current updates as appropriate.

- Device Health

Identifies devices that crash frequently, and therefore might need to be rebuilt or replaced and device drivers that are causing device crashes, with suggestions of alternative versions of those drivers that might reduce the number of crashes. Provides notification of Windows Information Protection misconfigurations that send prompts to end users.

Contoso has an existing Configuration Manager (Current Branch) infrastructure. Configuration Manager scales for large environments and provides extensive control over installation, updates, and settings. It also has built-in features to make it easier and more efficient to deploy and manage Windows 10 Enterprise.

Planning process

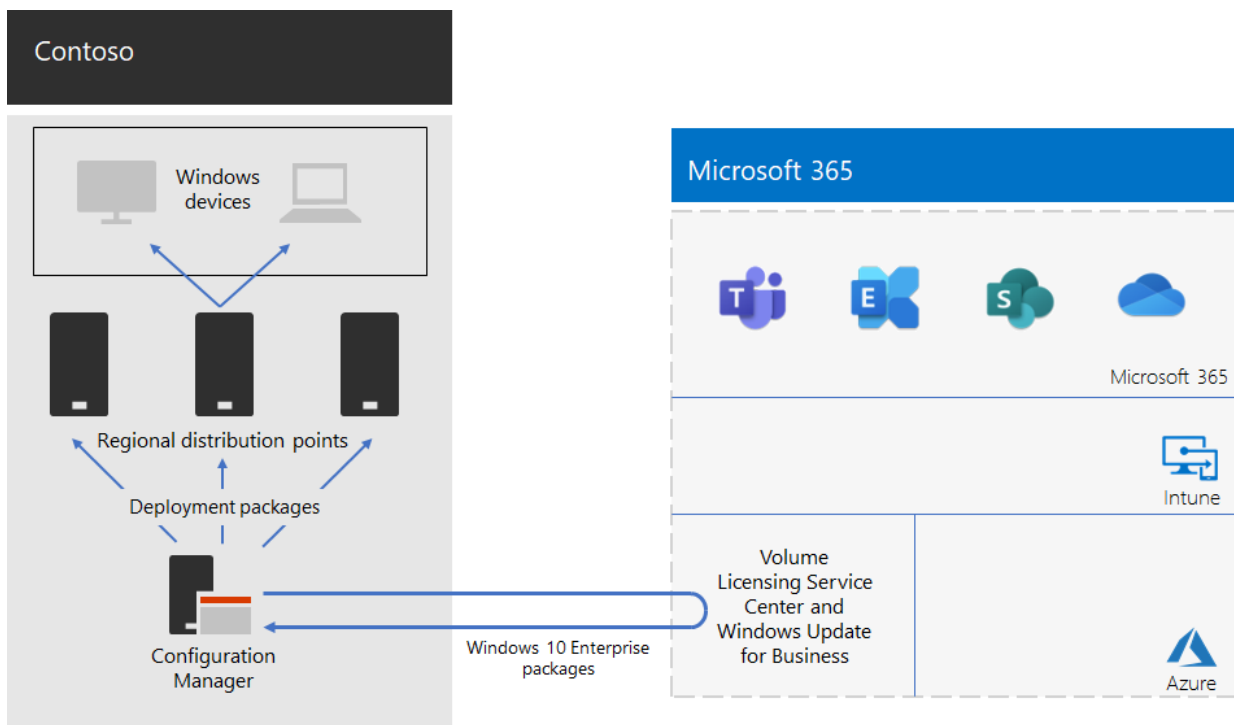
Contoso used the Upgrade Readiness in Windows Analytics to determine the set of installed apps and their compatibility with Windows 10 Enterprise.

Deployment process

To complete the in-place upgrade deployment of Windows 10 Enterprise, Contoso implemented the following process, which includes best practice recommendations from Microsoft:

1. Enabled peer cache for Configuration Manager.
2. Created customized Windows packages based on images from the Volume Licensing Service Center.
3. Used Configuration Manager to deploy the Windows packages to distribution points across their network and deployed builds to the three validation and deployment staging groups.
4. Performed assessment of success for PCs and devices in the three validation and deployment staging rings using the Device Health and Update Compliance solutions of Windows Analytics.
5. Based on the Windows Analytics information, Contoso determined the version of Windows 10 Enterprise to deploy to the broad deployment group.
6. Ran the Configuration Manager deployment task sequences to deploy the selected Windows package to the broad deployment group.
7. Monitored PCs and devices in the broad deployment group using the Device Health and Update Compliance solutions to address issues.

Here is Contoso's in-place upgrade and ongoing updates deployment architecture.



This infrastructure consists of:

- Configuration Manager, which:
 - Obtains images for Windows 10 Enterprise packages from the Microsoft Volume Licensing Center in the Microsoft Network.
 - Is the central administration point for deployment packages.
- Regional distribution points that are typically located in Contoso's regional hub offices.
- Windows PCs and devices in various locations that receive and install the deployment packages for the in-place upgrade or ongoing updates based on group membership.

Next step

Learn how Contoso is leveraging its Configuration Manager infrastructure to [deploy and keep current Microsoft 365 Apps for enterprise](#) across its organization.

See also

[Windows 10 Enterprise](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Microsoft 365 Apps for enterprise deployment for Contoso

10/28/2022 • 4 minutes to read • [Edit Online](#)

Contoso upgraded their PCs to Windows 10 Enterprise and Microsoft 365 Apps for enterprise to enable more effective collaboration, better security, and a more modern desktop experience. After they assessed their infrastructure and business needs, Contoso identified these key requirements for the deployment:

- All PCs should run Microsoft 365 Apps for enterprise.
- Deployment should use existing management tools and infrastructure when possible.
- Deployment must support multiple languages and existing architectures on users' devices.
- PCs should stay up-to-date and secure with minimal IT administrative costs and minimal impact to users.

Deployment tools

Based on their requirements, Contoso chose to deploy Windows 10 Enterprise and Microsoft 365 Apps for enterprise through Configuration Manager (Current Branch). Configuration Manager scales for large environments and provides extensive control over installation, updates, and settings. It also has built-in features to make it easier and more efficient to deploy and manage Office, including:

- Peer cache, which can help with limited network capacity when deploying to devices in remote locations.
- The Office Client Management dashboard, which makes it easy to deploy Office and monitor updates and gives administrators access to the latest deployment and management features.
- Intelligent language pack deployment, including automatically deploying the same language as the operating system.
- A fully supported and easy-to-use method of removing existing versions of Office from a client during deployment.

In addition to Configuration Manager, Contoso used the [Readiness Toolkit for Office Add-ins and VBA](#), a free tool from Microsoft, to assess compatibility issues with their Office macros and add-ins.

Managing deployment and updates

Microsoft 365 Apps for enterprise has a new release model: Office as a service. The service model makes it easy to stay up to date with new features. But it often requires IT departments to change how they deploy and test new releases. To minimize compatibility issues and to ensure their computers stay up to date, Contoso deployed Windows and Office in two stages:

- First, they deployed Microsoft 365 Apps for enterprise to a small set of representative devices across the organization. This pilot group was used to test apps, add-ins, and hardware with Microsoft 365 Apps for enterprise.
- Four months later, after addressing all critical issues with apps, add-ins, and hardware in the pilot group, Contoso deployed Microsoft 365 Apps for enterprise to the rest of the devices in the organization (the broad group).

Instead of managing updates to Office by using Configuration Manager, Contoso enabled automatic updates from the cloud. Cloud-based updates reduce administrative overhead while ensuring that devices stay up to date.

Contoso followed the same two-stage approach for feature updates as they used for deploying Office: Devices

in the pilot group received feature updates four months earlier than devices in the rest of the organization (the broad group). To enable this for Office, Contoso used two recommended [update channels](#):

- Semi-Annual Enterprise Channel (Preview) for updates to the pilot group
- Semi-Annual Enterprise Channel for updates to the broad group

Because the Semi-Annual Enterprise Channel (Preview) releases a version of Microsoft 365 Apps for enterprise four months earlier than the Semi-Annual Enterprise Channel, Contoso has time to validate the updates without having to manage them.

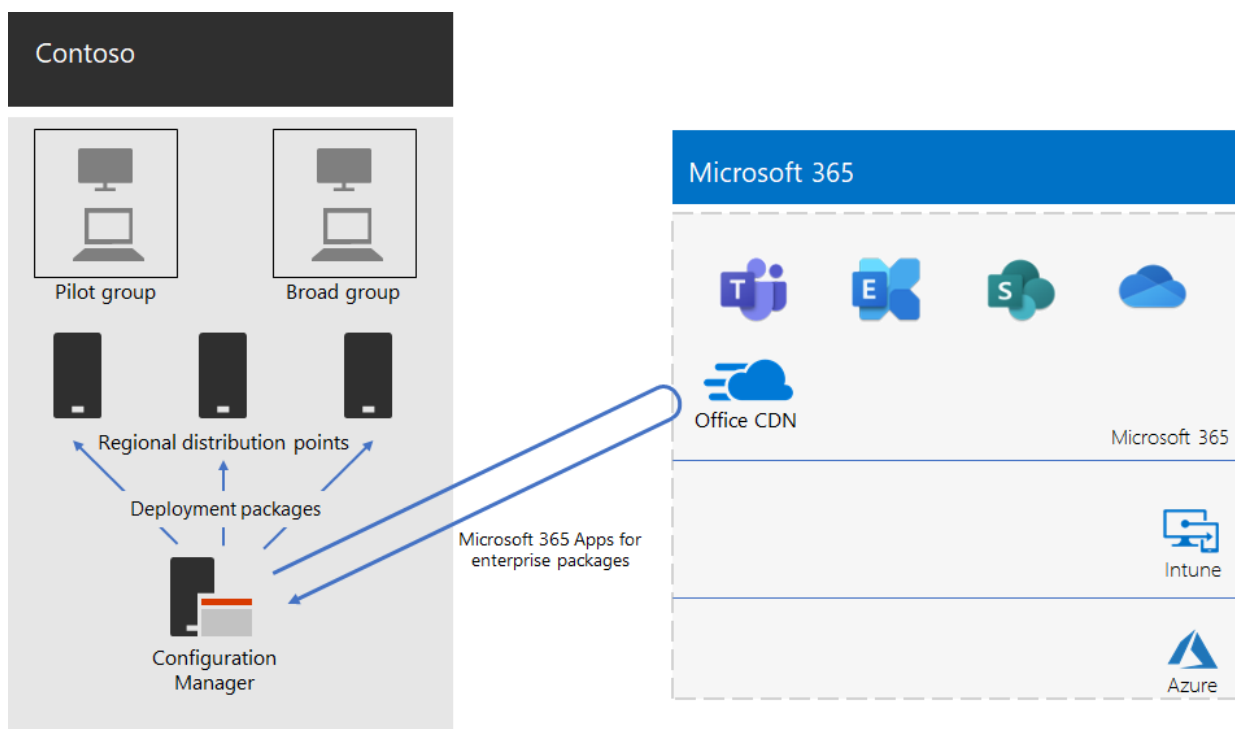
Deployment process

To complete the deployment of Office, Contoso implemented the following process, which includes best practice recommendations from Microsoft:

1. Before deployment, Contoso used the Readiness Toolkit for Office Add-in and VBA to test their apps and Office Add-ins to assess their compatibility with Microsoft 365 Apps for enterprise.
2. In Configuration Manager, they enabled peer cache on their client devices, which helps with limited network capacity when deploying to client devices in remote locations.
3. Contoso defined two deployment groups as device collections in Configuration Manager: a pilot group and a broad group. The pilot group, which included a small set of representative devices across the organization, was used for additional testing of apps, add-ins, and hardware with Windows 10 Enterprise and Microsoft 365 Apps for enterprise.
4. They created deployment packages for Office by using the Office Client Management dashboard and the Office 365 Installer wizard, which are both part of the Configuration Manager console. They built two Microsoft 365 Apps for enterprise packages, one for the pilot group on the Semi-Annual Enterprise Channel (Preview) and one for the broad group on the Semi-Annual Enterprise Channel.
5. Each Office package included English, French, and German Language packs. If a device required a language that wasn't included in the Office package, that language pack was automatically downloaded from the Office Content Delivery Network (CDN).
6. They used the built-in feature in the Office package to automatically remove all existing MSI versions of Office before installing Microsoft 365 Apps for enterprise.
7. In Configuration Manager, they deployed the Windows and Office packages to distribution points across their network. Then they ran the Configuration Manager deployment task sequences to deploy the pilot Microsoft 365 Apps for enterprise package to the pilot group.
8. After they addressed compatibility issues with the pilot group, Contoso ran the task sequences to deploy the Microsoft 365 Apps for enterprise package to the broad group.

Because Contoso chose to automatically update devices from the cloud, there was no need to manage the process in Configuration Manager. Their devices are automatically updated directly from the cloud-based on the update channel that was defined in the initial deployment.

Here is the Contoso Microsoft 365 Apps for enterprise installation and ongoing updates deployment architecture.



Next step

Learn how Contoso is [using Microsoft Intune](#) in Microsoft 365 for enterprise to manage its devices and the apps that they run across the organization.

See also

[Microsoft 365 Apps for enterprise](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Mobile device management for Contoso

10/28/2022 • 2 minutes to read • [Edit Online](#)

Microsoft 365 for enterprise includes Intune and a set of Azure services that support mobile device and application management and security.

Contoso has many mobile-enabled employees. Some have offices in Contoso locations, and some have no offices. Contoso needed a way to enable employee productivity but keep the devices, the Contoso data stored on those devices, and application behavior secure.

Plan

Contoso identified the following Intune use cases of mobile device management for Microsoft 365 for enterprise:

- Protect Exchange Online email and data so it can be safely accessed by mobile devices.
- Implement a bring-your-own-device (BYOD) program for Contoso employees.
- Issue organization-owned phones and limited-use shared tablets to Contoso employees.

Contoso doesn't use Intune to:

- Allow employees to securely access Microsoft 365 from an unmanaged public kiosk.
- Protect on-premises email and data so it can be safely accessed by mobile devices, because there are no on-premises Microsoft Exchange servers.

Deploy

This is how Contoso set up their mobile device management infrastructure:

- Set Intune as the Mobile Device Management (MDM) authority, and use Intune on Azure to administer content and manage the devices
- Created Azure Active Directory (Azure AD) groups for devices for enrollment and Intune settings and device-based Conditional Access policies

For more information, see [Contoso Conditional Access policies](#).

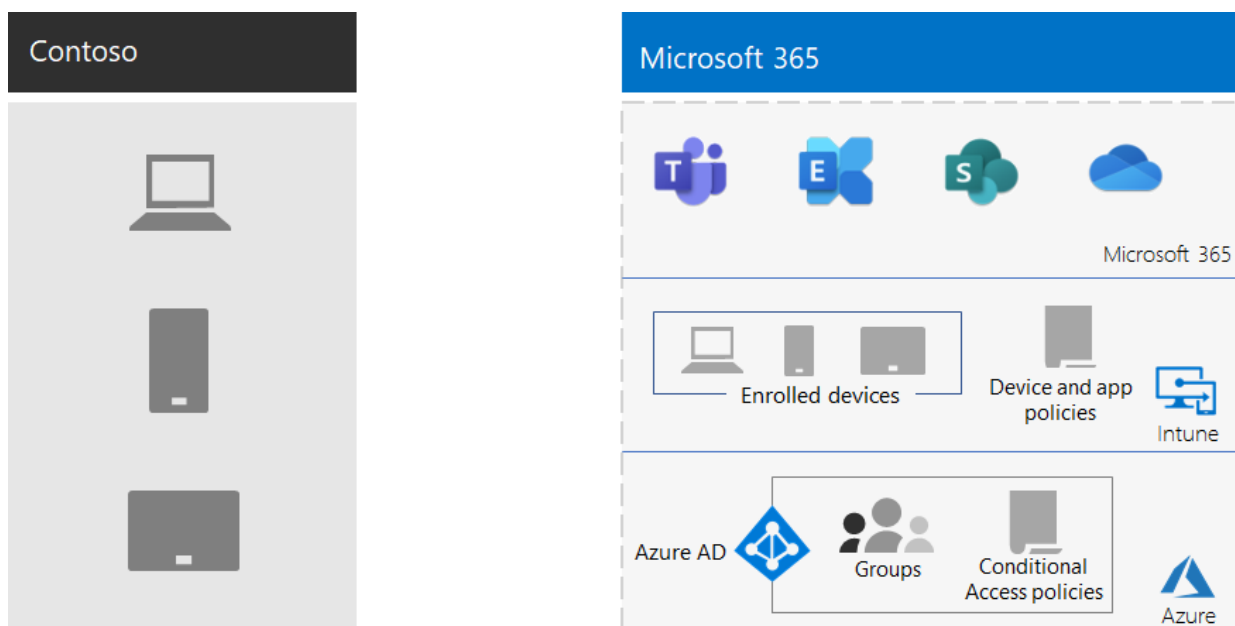
- Enabled the Apple device platform to support employees with iPads, iMacs, and iPhones, and corporate-owned iPhones
- Created Contoso-specific terms and conditions policies, which are seen during the installation of the Company Portal for Contoso on mobile devices
- For devices that aren't enrolled, implemented a set of Mobile Application Management (MAM) policies to require authentication for access to Microsoft 365 services
- Created Intune policies that enforce:
 - Allowed apps.
 - Device encryption to help prevent unauthorized access.
 - A six-digit PIN or password.
 - An inactivity-timeout period.
 - Antivirus and malware protection, and signature updates with Windows Defender on Windows 10

devices.

- Automatic updates on Windows 10 devices that include the latest security updates.
- Pushing certificates to managed devices.
- A clear separation of business and personal data. Users or admins can selectively wipe corporate data from the device, while leaving personal data such as pictures, personal email accounts, and personal files untouched.

Contoso enrolled deployed PCs and company-owned smartphones and tablets by adding them to the appropriate Intune device groups. They also established a BYOD program for employees to enroll their personal devices. Enrolled devices receive Intune policies, which result in managed and secured devices and their applications. Devices that aren't enrolled have Mobile Application Management (MAM) policies that specify allowed applications.

Here is the Contoso mobile device management deployment architecture.



Next step

Learn how Contoso uses the [information protection capabilities](#) of Microsoft 365 for enterprise to classify, identify, and protect crucial digital assets across its organization.

See also

[Device management for Microsoft 365](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Information protection for the Contoso Corporation

10/28/2022 • 4 minutes to read • [Edit Online](#)

Contoso is serious about their information security. Leakage or destruction of intellectual property that describes their product designs and proprietary manufacturing techniques would place them at a competitive disadvantage.

Before moving their sensitive digital assets to the cloud, Contoso made sure that their on-premises information classification and protection requirements were supported by the cloud-based services of Microsoft 365 for enterprise.

Contoso data security classification

Contoso performed an analysis of their data and determined the following classification levels.

LEVEL 1: BASELINE	LEVEL 2: SENSITIVE	LEVEL 3: HIGHLY REGULATED
Data is encrypted and available only to authenticated users. Provided for all data stored on-premises and in cloud-based storage and workloads. Data is encrypted while it resides in the service and in transit between the service and client devices. Examples of Level 1 data are normal business communications (email) and files for administrative, sales, and support workers.	Level 1 plus strong authentication and data loss protection. Strong authentication includes Azure AD Multi-Factor Authentication (MFA) with SMS validation. Microsoft Purview Data Loss Prevention ensures that sensitive or critical information doesn't travel outside the Microsoft cloud. Examples of Level 2 data are financial and legal information and research and development data for new products.	Level 2 plus the highest levels of encryption, authentication, and auditing. The highest levels of encryption for data at rest and in the cloud, compliant with regional regulations, combined with MFA with smart cards and granular auditing and alerting. Examples of Level 3 data are customer and partner personal information, product engineering specifications, and proprietary manufacturing techniques.

Contoso information policies

The following table lists the Contoso information policies.

VALUE	ACCESS	DATA RETENTION	INFORMATION PROTECTION
Low business value (Level 1: Baseline)	Allow access to all.	6 months	Use encryption.
Medium business value (Level 2: Sensitive)	Allow access to Contoso employees, subcontractors, and partners. Use MFA, Transport Layer Security (TLS), and Mobile Application Management (MAM).	2 years	Use hash values for data integrity.

VALUE	ACCESS	DATA RETENTION	INFORMATION PROTECTION
High business value (Level 3: Highly regulated)	Allow access to executives and leads in engineering and manufacturing. Rights Management System (RMS) with managed network devices only.	7 years	Use digital signatures for non-repudiation.

The Contoso path to information protection with Microsoft 365 for enterprise

Contoso followed these steps to prepare Microsoft 365 for enterprise for their information-protection requirements:

1. Identify what information to protect

Contoso did an extensive review of their existing digital assets located on on-premises SharePoint sites and file shares and classified each asset.

2. Determine access, retention, and information protection policies for data levels

Based on the data levels, Contoso determined detailed policy requirements, which were used to protect existing digital assets as they were moved to the cloud.

3. Create sensitivity labels and their settings for the different levels of information

Contoso created sensitivity labels for their data levels, with their highly regulated label that includes encryption, permissions, and watermarks.

4. Move data from on-premises SharePoint sites and file shares to their new SharePoint sites

The files migrated to the new SharePoint sites inherited the default retention labels assigned to the site.

5. Train employees how to use sensitivity labels for new documents, how to interact with Contoso IT when creating new SharePoint sites, and to always store digital assets on SharePoint sites

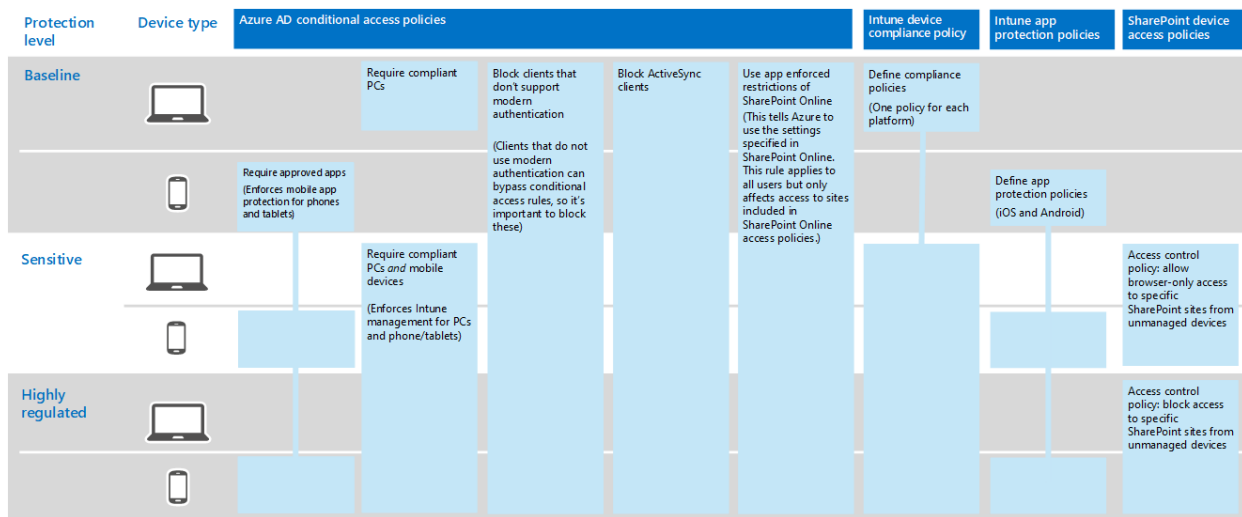
Changing bad worker information-storage habits is often considered the hardest part of the information protection transition for the cloud. Contoso IT and management needed to get employees to always label and store their digital assets in the cloud, refrain from using on-premises file shares, and not use third-party cloud storage services or USB drives.

Conditional Access policies for information protection

As part of their rollout of Exchange Online and SharePoint, Contoso configured the following set of Conditional Access policies and applied them to the appropriate groups:

- [Managed and unmanaged application access on devices policies](#)
- [Exchange Online access policies](#)
- [SharePoint access policies](#)

Here's resulting set of Contoso policies for information protection.



NOTE

Contoso also configured additional Conditional Access policies for identity and sign-in. See [Identity for the Contoso Corporation](#).

These policies ensure that:

- Apps that are allowed and the actions they can take with the organization's data are defined by app protection policies.
- PCs and mobile devices must be compliant.
- Exchange Online uses Office 365 message encryption (OME) for Exchange Online.
- SharePoint uses app-enforced restrictions.
- SharePoint uses access control policies for browser-only access and to block access for unmanaged devices.

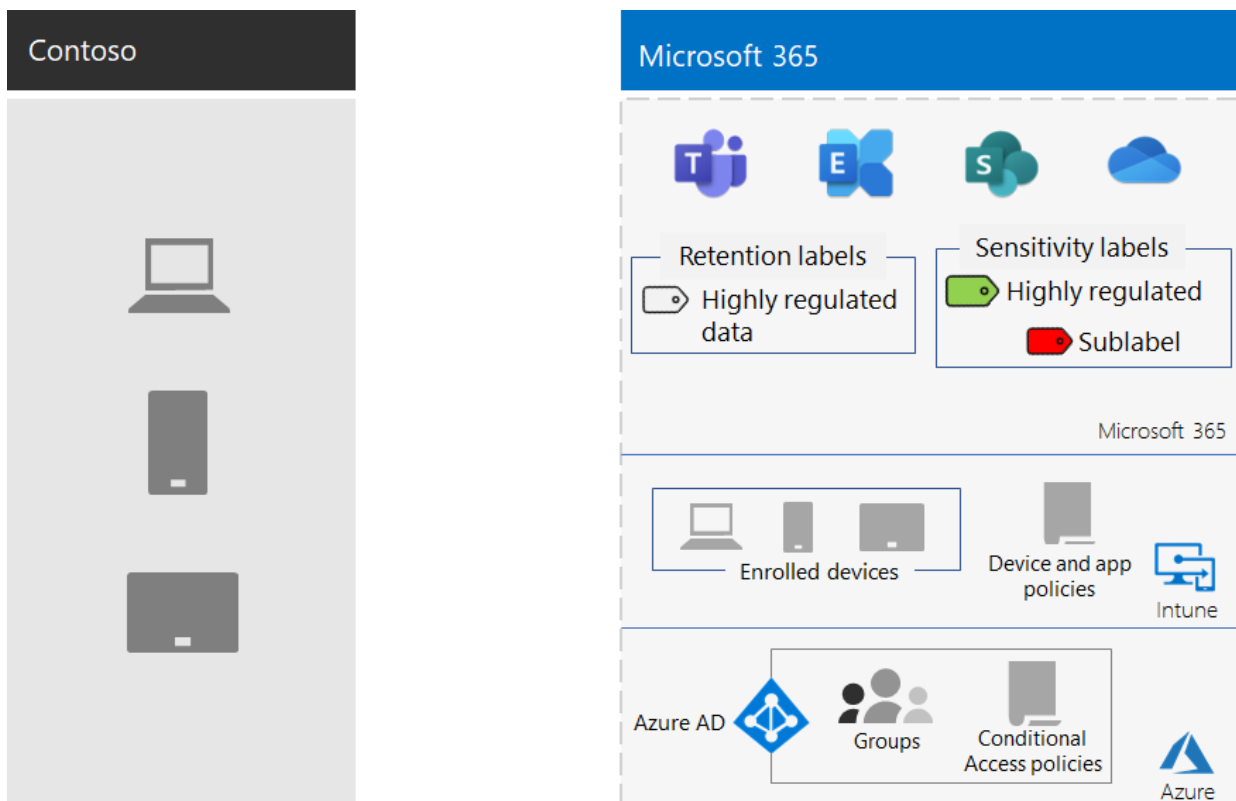
Mapping Microsoft 365 for enterprise features to Contoso data levels

The following table maps Contoso data levels to information protection features in Microsoft 365 for enterprise.

LEVEL	MICROSOFT 365 CLOUD SERVICES	WINDOWS 10 AND MICROSOFT 365 APPS FOR ENTERPRISE	SECURITY AND COMPLIANCE
Level 1: Baseline	SharePoint and Exchange Online Conditional Access policies Permissions on SharePoint sites	Sensitivity labels BitLocker Windows Information Protection	Device Conditional Access policies and Mobile Application Management policies
Level 2: Sensitive	Level 1 plus: Sensitivity labels Microsoft 365 retention labels on SharePoint sites Data Loss Prevention for SharePoint and Exchange Online Isolated SharePoint sites	Level 1 plus: Sensitivity labels on digital assets	Level 1

LEVEL	MICROSOFT 365 CLOUD SERVICES	WINDOWS 10 AND MICROSOFT 365 APPS FOR ENTERPRISE	SECURITY AND COMPLIANCE
Level 3: Highly regulated	Level 2 plus: Bring your own key (BYOK) encryption and protection for trade secret information Azure Key Vault for line-of-business applications that interact with Microsoft 365 services	Level 2	Level 1

Here's the resulting Contoso information-protection configuration.



Next step

Learn how Contoso uses the [security features across Microsoft 365 for enterprise](#) for identity and access management, threat protection, information protection, and security management.

See also

[Microsoft Defender for Office 365](#)

[Microsoft 365 for enterprise overview](#)

[Test lab guides](#)

Summary of Microsoft 365 for enterprise security for the Contoso Corporation

10/28/2022 • 5 minutes to read • [Edit Online](#)

To get approval to deploy Microsoft 365 for enterprise, the Contoso IT security department conducted a thorough security review. They identified the following security requirements for the cloud:

- Use the strongest methods of authentication for employee access to cloud resources.
- Ensure that PCs and mobile devices connect and access applications in secure ways.
- Protect PCs and email from malware.
- Permissions on cloud-based digital assets define who can access what and what they can do, and are designed for least-privilege access
- Sensitive and highly regulated digital assets are labeled, encrypted, and stored in secure locations.
- Highly regulated digital assets are protected with additional encryption and permissions.
- IT security staff can monitor the current security posture from central dashboards and get notified of security events for quick response and mitigation.

The Contoso path to Microsoft 365 security readiness

Contoso followed these steps to prepare their security for their deployment of Microsoft 365 for enterprise:

1. Limit administrator accounts for the cloud

Contoso did an extensive review of its existing Active Directory Domain Services (AD DS) administrator accounts and set up series of dedicated cloud administrator accounts and groups.

2. Classify data into three security levels

Contoso did a careful review and determined the three levels, which were used to identify the Microsoft 365 for enterprise features to protect the most valuable data.

3. Determine access, retention, and information protection policies for data levels

Based on the data levels, Contoso determined detailed requirements to qualify future IT workloads that are moved to the cloud.

To follow security best practices and Microsoft 365 for enterprise deployment requirements, Contoso security administrators and its IT department deployed many security features and capabilities, as described in the following sections.

Identity and access management

- Dedicated global administrator accounts with MFA and PIM

Rather than assign the global admin role to everyday user accounts, Contoso created three dedicated global administrator accounts with strong passwords. The accounts are protected by Azure AD Multi-Factor Authentication (MFA) and Azure Active Directory (Azure AD) Privileged Identity Management (PIM). *PIM is only available with Microsoft 365 E5.*

Signing in with a **Azure AD DC admin**, or **Global admin** account is only done for specific administrative tasks. The passwords are only known to designated staff and can only be used within a time period that's configured in Azure AD PIM.

Contoso security administrators assigned lesser admin roles to accounts that are appropriate to that IT worker's job function.

For more information, see [About Microsoft 365 admin roles](#).

- MFA for all user accounts

MFA adds an additional layer of protection to the sign-in process. It requires users to acknowledge a phone call, text message, or app notification on their smart phone after correctly entering their password. With MFA, Azure AD user accounts are protected against unauthorized sign-in, even if an account password is compromised.

- To protect against compromise of the Microsoft 365 subscription, Contoso requires MFA on all **Azure AD DC admin**, or **Global admin** accounts.
- To protect against phishing attacks, in which an attacker compromises the credentials of a trusted person in the organization and sends malicious emails, Contoso enabled MFA on all user accounts, including managers and executives.

- Safer device and application access with Conditional Access policies

Contoso is using [Conditional Access policies](#) for identity, devices, Exchange Online, and SharePoint. Identity Conditional Access policies include requiring password changes for high-risk users and blocking clients from using apps that don't support modern authentication. Device policies include the definition of approved apps and requiring compliant PCs and mobile devices. Exchange Online Conditional Access policies include blocking ActiveSync clients and setting up Office 365 message encryption. SharePoint Conditional Access policies include additional protection for sensitive and highly regulated sites.

- Windows Hello for Business

Contoso deployed [Windows Hello for Business](#) to eventually eliminate the need for passwords through strong two-factor authentication on PCs and mobile devices running Windows 10 Enterprise.

- Windows Defender Credential Guard

To block targeted attacks and malware running in the operating system with administrative privileges, Contoso enabled [Windows Defender Credential Guard](#) through AD DS group policy.

Threat protection

- Protection from malware with Microsoft Defender Antivirus

Contoso is using [Microsoft Defender Antivirus](#) for malware protection and anti-malware management for PCs and devices running Windows 10 Enterprise.

- Secure email flow and mailbox audit logging with Microsoft Defender for Office 365

Contoso is using Exchange Online Protection and [Defender for Office 365](#) to protect against unknown malware, viruses, and malicious URLs transmitted through emails.

Contoso also enabled mailbox audit logging to identify who logs in to user mailboxes, sends messages, and does other activities performed by the mailbox owner, a delegated user, or an administrator.

- Attack monitoring and prevention with Office 365 threat investigation and response

Contoso uses [Office 365 threat investigation and response](#) to protect users by making it easy to identify and address attacks, and to prevent future attacks.

- Protection from sophisticated attacks with Advanced Threat Analytics

Contoso is using [Advanced Threat Analytics \(ATA\)](#) to protect itself from advanced targeted attacks. ATA

automatically analyzes, learns, and identifies normal and abnormal entity (user, devices, and resources) behavior.

Information protection

- Protect sensitive and highly regulated digital assets with Azure Information Protection labels

Contoso determined three levels of data protection and deployed [Microsoft 365 sensitivity labels](#) that users apply to digital assets. For its trade secrets and other intellectual property, Contoso uses sensitivity sublabels for highly regulated data. This process encrypts content and restricts access to specific user accounts and groups.

- Prevent intranet data leaks with Data Loss Prevention

Contoso configured [Microsoft Purview Data Loss Prevention](#) policies for Exchange Online, SharePoint, and OneDrive for Business to prevent users from accidentally or intentionally sharing sensitive data.

- Prevent device data leaks Windows Information Protection

Contoso is using [Windows Information Protection \(WIP\)](#) to protect against data leakage through internet-based apps and services and enterprise apps and data on enterprise-owned devices and personal devices that employees bring to work.

- Cloud monitoring with Microsoft Defender for Cloud Apps

Contoso is using [Microsoft Defender for Cloud Apps](#) to map their cloud environment, monitor its usage, and detect security events and incidents. *Microsoft Defender for Cloud Apps is only available with Microsoft 365 E5.*

- Device management with Microsoft Intune

Contoso uses [Microsoft Intune](#) to enroll, manage, and configure access to mobile devices and the apps that run on them. Device-based Conditional Access policies also require approved apps and compliant PCs and mobile devices.

Security management

- Central security dashboard for IT with Microsoft Defender for Cloud

Contoso uses the [Microsoft Defender for Cloud](#) to present a unified view of security and threat protection, to manage security policies across its workloads, and to respond to cyberattacks.

- Central security dashboard for users with Windows Defender Security Center

Contoso deployed the [Windows Security app](#) to its PCs and devices running Windows 10 Enterprise so that users can see their security posture at a glance and take action.

Microsoft 365 documentation navigation guide

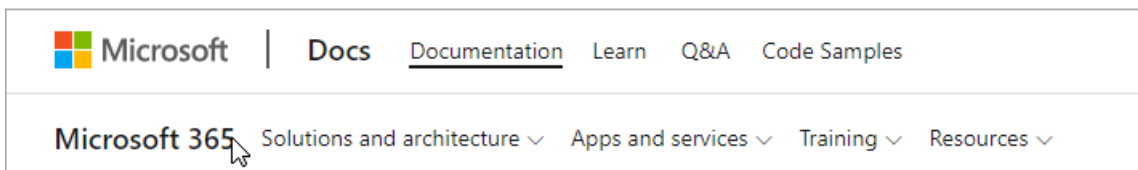
10/28/2022 • 2 minutes to read • [Edit Online](#)

This topic provides some tips and tricks for navigating the Microsoft 365 technical documentation space.

Hub page

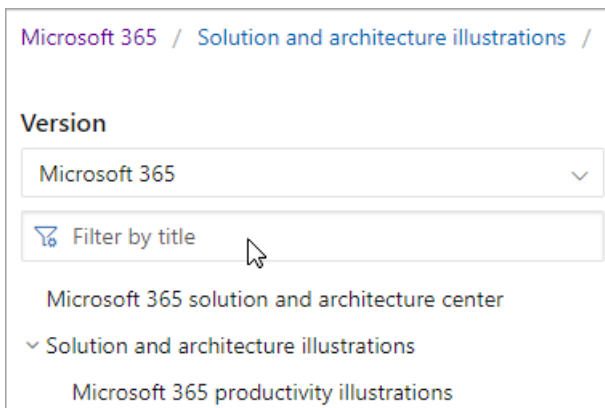
The Microsoft 365 hub page can be found at <https://aka.ms/microsoft365docs> and is the entry point for finding relevant Microsoft 365 content.

You can always navigate back to this page by selecting **Microsoft 365** from the header at the top of every page within the Microsoft 365 technical documentation set:



TOC search

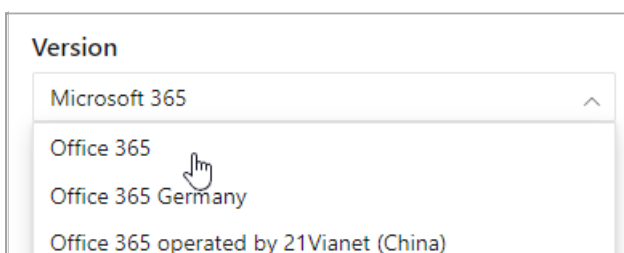
On Microsoft Learn, you can search the content in the table of contents by using the filter search box at the top:



Version filter

The Microsoft 365 technical documentation provides content for additional products, including Office 365 Germany and Office 365 operated by 21 Vianet (China). Features can vary between these versions, and as such, sometimes the content itself can vary.

You can use the version filter to ensure that you are seeing content for the appropriate version of Microsoft 365:



Breadcrumbs

Breadcrumbs can be found below the header and above the table of contents, and indicate where the current article is located in the table of contents. Not only does this help set the context to what type of content you're reading, but it also allows you to navigate back up the table of contents tree:

[Microsoft 365](#) / [Microsoft 365 security](#) / [Microsoft 365 Defender](#) / [Plan](#) / [Data security and privacy](#)

Article section navigation

The right-hand navigation pane allows you to quickly navigate to sections within an article, as well as identify your location within the article.

Is this page helpful?
 Yes No

In this article

- Step 1: Set up multi-factor authentication and conditional access policies**
- Step 2: Configure Microsoft Defender for Identity
- Step 3: Turn on Microsoft 365 Defender
- Step 4: Configure Microsoft Defender for Office 365
- Step 5: Configure Microsoft Defender for Endpoint
- Step 6: Configure Microsoft Cloud App Security
- Step 7: Monitor status and take actions
- Step 8: Train users

Submit feedback

If you find something wrong within an article, you can submit feedback to the SQL Content team for that article by scrolling down to the bottom of the page and selecting **Content feedback**.

Feedback

Submit and view feedback for

[This product](#)

[This page](#)

Contribute to Microsoft 365 documentation

Did you know that you could edit the content on Microsoft Learn yourself? If you do so, not only will our documentation improve, but you'll also be credited as a contributor to the page. To get started, see:

- [Microsoft Docs contributor guide](#)

Next steps

- Get started with the [Microsoft 365 technical documentation](#).

